Q&A Pod Transcript
ICANN73 Plenary Session: Evolving the DNS Abuse Conversation
Wednesday, 9 March 2022 10:30-12:00 AST

1. I hope that this will be covered, but if not, do we know roughly the ration of hacked vs malicious registration?, *Alan Greenberg*

   - Answered live.

2. Can we use AI-based tools to differentiate between the 2 cases?, *Mouloud Khelif – ICANN73 Fellow*

   - Answered live.

3. How could this (wp-include) happened when the HTTPS is used ?, *Olevie A. A. Kouami*

   - HTTPS does not prevent compromise.

4. There are three types of compromise.
   1. Web server compromise
   2. Authoritative DNS sever compromise
   3. Registration data compromise

   We also have to distinguish these three types as well., *Yoshiro Yoneya*

5. How does abuse at the mail server level fit in to your proposed approach?, *Gregory Shatan*

   - Answered live.

6. May be slightly out of scope for this session, but curious what happens when a threat entity registers and builds a legitimate domain with the intent to use it in a valid manner for real business purposes, while also knowingly performing and masking illicit activities taking place in other portions of the domain. Some sources are seeing an increase in this type of activity, which suggests a third option for the final decision point on your flow chart, and more difficult to investigate and take action…, *Dan Owen*

7. Maciej, well done. Robust methodology and good call on calling out the limitations of the method. I was wondering if the ML method and the features used in COMAR also includes some of those heuristics you pointed out in the first method. If so, which ones as examples., *Samaneh Tajalizadeh, ICANN Org*

   - Answered live.

8. I would appreciate Maciej opinion on the high percentage of compromised domain names within European ccTLDs, would this not likely be attributed to a growing number of European ccTLD doing identity checks. It is easier for malicious individuals to compromise a domain/website as opposed to register a domain name with fraudulent or synthetic registrant data?, *Michael Palage*

   - Answered live.

9. Further to a question in the chat from Gabriel Andrews (PSWG), are there public user-friendly tools that (even non-technical) end users can use to assess if domains under their control have been compromised (and possibly who to contact to address any such compromise)?, *Brian Beckham*

   - the RrSG is working on such a tool as is Graeme's DNSAI; currently, the user would have to google for "who is the hosting company" although even once we've created these tools promulgation may be an issue

10. For the study, the time between registration and blacklist was used to differentiate between malicious and hacked. I don't understand how timing helps determine the category prior to blacklisting., *Jonathan Zuck*

11. Has there been any thought of looking at what percentage of infringing names are used to perpetrate abuse?, *Elisa Cooper*

12. What made you determine trademark infringement is DNS abuse?
    does this term refer to
    a) infringement by the domain name
    b) infringement in the content
    c) both
    Volker Greimann (RRSG)

    - Definitions are out of scope for today

13. Does the AI distinguish Malicious registrations such as the paypal examples versus Registrations that are done for click/forwarding purposes?, *Fernando España (.US)*

14. In cases where there is DNS abuse far more than in excess of 'tolerable' abuse, does ICANN reach out to the ccManager and ask for affirmative action of some kind, such as ask for a cleanup / change of management or change of status as a cc?, *Sivasubramanian M*

    - ICANN has no authority over CCs, but I think that's a question for another session.

15. Comment:

You're conflating domain registrations with DNS records
The paypal example was not a registration but a DNS record, *Michele Neylon (Blacknight)*

- Thanks Michele

16. For cases that abused domains cannot be easily determined to be compromised or maliciously registered (e.g. that receive borderline score by AI detection system), currently are there processes to determine the nature of the domain statuses and having certain actions for these (temporary) undetermined cases?, *Shih-Shiuan Kao*

    - My sense is that there is very little AI actually implemented. Most Rrs will default here to being cautious and treating as a comp. website.

17. I'm curious how people deal with automated reports (aka netcraft for example) that go and report a single 'parked' compromise across all domains pointing to that parked server, and demanding that every domain name parked there, be taken down..., *Calvin Browne*

    -apologies – pressed the wrong button . So Donuts has automated reports from Netcraft - and we apply our evidence based review of the report. If it doesn't objectively come with evidence, there is very little we, as a registry can do. But we take all reports, and will review them all as them come in.

18. Fully agree that these two types of abuse need to be distinguished. However, I would appreciate panelist feedback regarding the importance of accurate registrant data to either more quickly identify a malicious domain name registration or to get in contact with a compromised domain name to help them resolve the security issue., *Michael Palage*

    - Thanks Michael. considering the point of escalation here from a RY is to the registrar - who can then test current accuracy requirements pretty easily. I'm not sure of the tie.

    This would be similiar in may escalation paths - to the regsitrar - contact with the regsitrant is key.

    To the hosting company - well the regsitrant is somewhat moot - as it's a layer down.

19. Building on prior question, what role does ICANN play here when registrars don't do all the great stuff being discussed here and would changes to the RAA help bring those "bad registrars" into line with the best practices discussed here today?, *Fabricio Vayra*

- Answered live.

20. <comment>DNS abuse at a website level where the domain name is maliciously registered is often a short-term registration (1 year). The non-renewals in some of the new gTLDs that see a lot of problem registrations due to heavy discounting can be has high as 95%. It is important to differentiate compromised sites from other types of sites.</comment>?, John McCormac – HosterStats.com

    - Thank you John.

21. My biggest problem with making the distinction up front is the timing to actual mitigation. it seems as though these attacks are fast and require fast mitigation. My guess is that the whole attack is over before we've even figured out the "blame.", *Jonathan Zuck*

    - My sense is that building expertise on the distinction speeds up mitigation, rather than slows it down.

22. <comment>Some forms of compromise have secondary signs of compromise such as an out of date Wordpress or Joomla installation and a link injection compromise.</comment>, John McCormac – HosterStats.com

    - Thank you John.

23. It seems ICANN's Contractual Compliance dept. already make the distinction proposed in Graeme's process flowchart? Many tickets re: abuse are closed as out of ICANN's remit., *J-P Voilleque – ICANN Wiki*

24. How can we make sure that DNS abuse is preventative and make sure that someone is held accountable? *James Paek*

    - Thank you James, I think this is a bigger question than we can answer here today.

25. It seems that most of the decision making and corresponding actions on a compromised domain are being done at the DNS level. From my experience, webhosting providers can do a lot in that regard (and have done so in many occasions). Is there an effort to communicate/coordinate with them?, *Ahmad Aghar – ICANN73 Fellow*

    - Thanks Ahmad, I think we've answered this.

26. What is helpful to include in an abuse report to trigger these great mitigation tactics discussed here and should there be a uniform submission process (and how do we get uniformity in the ecosystem -- seems like ICANN should play a role)?, *Fabricio Vayra*

- There isn’t a uniform process now and there should be. ICANN (as in the entire community including Org) has a role, but not the full responsibility here. Please see SAC115 (https://www.icann.org/en/system/files/files/sac-115-en.pdf) for an in-depth analysis on this important topic space.

27. In addition, is there a process where decision maker determines whether DNS abuse is actually abuse or not and how they move forward with the process to suspend the DNS entirely?, *James Paek*

28. Seems that there is generally agreement that maliciously registered v. compromised is a reasonable categorization and that each category demands distinct mitigation and escalation pathways. How do we go from acknowledging this to establishing standard and enforceable practices and obligations applicable to all Rr and Ry under the ICANN umbrella, and include as well actors outside direct ICANN umbrella, e.g. hosts, in this process?, *Griffin Barnett*

    - Answered live.

29. At present a Registry "maintains" A records for a registered domain name, but does not act a "root gateway" for that domain name? The question has multiple implications, raised here without a thought at the moment., *Sivasubramanian M*

    - Registries list the authoritative nameservers for domain names in their zone files, not A records. This literally does provide the “next level up” from the TLD itself in the DNS resolution process and the TLD itself is listed in the root zone. Nameserver records included in the zone will tie namerserver names to IP addresses, but those records don’t seem to be what you are referring to. So not sure this question is appropriately phrased. Could you restate?

30. Question: I think we need a DNS Abuse Response Playbook, for gTLD and ccTLD, with best practice, step by step, who is on the hook to develop that playbook?, *Jacques Latour*

    - I think, actually, that’s me!