Q&A Pod Transcript
Plenary Session: DNS Abuse and Malicious Registrations During COVID-19
Monday, 22 June 2020 13:00-14:30 (UTC+8)

1,"What is considered a ""non material"" amount of abuse vs. ""material"" amount of abuse?" Lori Schulman, live answered,
"First you have to be careful about what you consider “material abuse”. The definition of DNS abuse offers one view of “what”, but since nobody controls the malefactors, in particular registries and registrars, you can hit a “threshold” every month in a row and yet it would not be meaningful because it’s different malefactors each month." Lori - consider that poor phrasing on my part. I would maybe re-phrase as: we saw very low amounts of abusive registrations in both absolute and relative numbers.,"Here too at PIR - 14,700 domain names with Covid/Corona related terms in the registration, a total of 13 domain names suspended for either DNS Abuse or instances of things like fake cures/vaccines"

2, How is the cooperation from LEA in countries outside the US and EU? Dave Kissoondoyal
I'll try and share my perspective on this in the next section of the plenary.,"Our experience at Afilias has been good. We have relationships with a number of LEA outside of EU and the US. These are specific to a TLD, i.e., as a service provider, some of the TLDs we host operate primarily in non-US and non-EU jurisdictions and they choose to support their local LEA. We cooperate as directed by these registry operators within their TLD."

3, What exactly is the formal procedure to be followed for taking down the DNS which is confirmed as spam/abusive? Shradha Pandey
"Once a domain is confirmed for DNS Abuse, typically at the Registry level we will work with the Registrar who might apply clienthold (suspend) and if not, we would likely act at the Registry level and apply serverhold","There is no agreed standard formal procedure, although Spec 11 3(b) of the latest registry agreement for gTLDs has a framework defined for what happens by whom and when."

4, Question for Laureen - Does the “Websites” category include fraud on social media platofrms?,James Bladel
I believe so.

5,"Comment - would love to engage in discussion on the underlying issues: The statements by contracted parties that there was not a lot of domain registration abuse tied to COVID is not accurate in aggregate. From individual entities’ perspectives, this was the case, but not overall. Many bad actors switched to COVID themes during the current pandemic, and this has been reported widely in the security press. The discrepancy seems to be that the people who are saying that there wasn’t a lot of COVID related DNS Abuse (CENTR, Tucows, Afilias, and many others) are already very GOOD actors in this space and do not see a lot of such activities themselves since they prevent and quickly react to issues. That’s great, but this unfortunately creates a

false narrative that COVID didn’t lead to DNS Abuse. There are poor actors in the space where activities occurred, and a more accurate picture needs to be presented to better reflect where such issues have occurred, so we can mitigate problem provider issues." Rod Rasmussen
"The distinction I am making, which I believe is agreed by quite a number of CPH, is that the COVID problem is a website content abuse problem not a DNS abuse problem. This distinction between DNS versus website content is essential to the discussion of mitigation options."

6, AKA - the problem providers aren’t here and aren’t publishing studies on how bad their problems were/are.,Rod Rasmussen
"Hi Rod, you might be interested in teh Dynamic Coalition on Data and Trust. Giovanni Seppia is gathering interested parties and has a drfat proposal. Doesn't solve the issue of bad actors not sharing data, but at least will give us a platform to help us to be consistent with what we share."

7,"Q to the previous speaker: Have the Agencies considered the possibility of designing a secure process to actually channellise the relief disbursements through the perhaps making use of existing and new DNS technologies such as a blockchain based payment gateway, not only for the US, but usable elsewhere?" Anonymous Attendee
live answered

8, Thanks @Graeme ,Dave Kissoondoyal
live answered

9, Thanks Jim for the answer, Dave Kissoondoyal
live answered,,,

10, Thanks @ Brian. So the Registrar has to record his reasons for applying the clienthold(suspension)? Are these reasons mandatorily provided to the person whose DNS is suspended? Shradha Pandey
"Typically yes, the Registrar will notify the Registrant, if for no other reason that it/she/he is the customer of the Registrar. If a Registry takes action, we always notify the Registrar with the expectation that they notify the Registrant."

11,"Question for Jonathan - Given that Registries, Registrars, ICANN and even some LEAs demonstrate that less than 1% of COVID domains are abusive, how do you support the 50% claim?" James Bladel
"Well, James, what I said was that COVID related domains were 50% more likely to be abusive. That doesn’t mean 50% of them were abusive which was, of course, not the case. That said, the numbers are probably higher than you imagine because of the time lag associated with the study. abusive sites do NOT stay up very long for. this very reason."

12,"... ... disbursements through the DNS, perhaps utilizing existing and new technologies ... (typo)" Anonymous Attendee

live answered,,,

13,"<Question> Is it possible that some COVID-related registrations were benign because they were investigated after the fraud already occurred and the fraudsters ""folded shop"" and moved on? Do we have any data indicating otherwise?"" <Question>" Fabricio Vayra
"Good quesiton Fab, that would be possible for a few days at a time, but our practices at least would catch those “dormant” domains after they engage in DNS Abuse after a few days - it’s not like if they aren’t flagged as abusive on the first try it will never pop up on our radar"

14,"Ohh, that's interesting! Is there a fixed process for appealing against the decision of the Registrar if the customer believes that the registrar has made a mistake in his assessment?" Shradha Pandey
"Good question! It would not be uniform, it would be something you’d have to reach out to each Registrar or Registry"

15,"'@Jim - definitions here suck. DNS abuse vs. content abuse. For me, if the domain is registered for an abusive purpose, regardless of what the abuse is, it’s DNS abuse - some of which may be actionable depending on what the legalities are. If a website is compromised or has an “evil” user abusing it, then that’s “content abuse”. We’ve created this artificial contrivance of definitions that only apply to ICANN-land and nowhere else. Taxonomy matters and we suck at it right now…" Rod Rasmussen
"Definitions may “suck” but they server to clearly define the boundaries regarding who can mitigate and what mitigation can be done. Even among registries and registrars, what happened during COVID is that for domain names that were used obviously and egregiously only for abusive purposes, I.e., your definition, they were taken down. Other than that, nobody really wants to be the content police of the Internet. That’s the problem that’s hard to solve."

16,"'@ Brian , if it is not uniform, does it imply that there is a possibility that some Registrar or Registry might not have a process for appeal at all?" Shradha Pandey
"That’s possible Shradha, but I couldn’t speak for all Registries or Registrars",,,

17,"Thanks, Brian. How about the other way around? Meaning, they are dormant by the time they are checked, because the fraud already occured and the domain isn't used again after the check?" Fabricio Vayra
"Well then it would likely probably come to analysis of evidence gathered, things like screenshots of the phish/fraud perptrated."

18,"Just trying to make sense of the high level of registrations, the abuse reported widely and the low level of actionable abuse reported here by contracted parties." Fabricio Vayra
"This is an important dialogue to have Fab. Some behaviors we can all agree are abusive and they tend to be straightforward to mitigate. But there is still a good deal of abuse that is only abusive in some contexts and not others. How we adjudicate that can

be a real problem. Not all TLDs are created equal and speaking as a service provider for over 200 TLDs, I can tell you we serve the needs of our customers and they vary. I think a minimum is well defined. You may disagree."

19,"Pretty big spread between 50% and 1%. The vast majority (70%) of COVID/CORONA registrations are inactive, and likely defensive." James Bladel
"I'm not sure parked is necessarily defensive, in this case, but dormant. These sites not live for very long."

20, Thanks @ Brian, Shradha Pandey
"Sure thing, Shradha!",,,

21,"<Question> Voluntary measures are a good start, but not the long-term answer. How do we ensure that some registrars don't carry the weight for all and level the playing field through proactive data driven contract comapliance? Seems as thought through contract compliance we address those bad actors we are all talking about that are ""not in the room."" <Question>", Fabricio Vayra
live answered

22,"Thanks, James.
<Question> So how can we be proactive – not reactive -- using some of the methods we're all saying worked well in response to COVID registrations? How do we use those learned experiences and prepare for the next crisis (e.g., the next Hurricane, Earthquake, Pandemic, etc.). It seems the abuse is cyclical and bad actors aren't going to stop leveraging the DNS, so why not prepare a system to address the abuse in advance? <Question>", Fabricio Vayra
"To be honest Fab, from my point of view, there was nothing special about COVID. We used ordinary every day processes and did what we did. We went back and pulled out counts of COVID related registrations to find that out of about 5000 registrations we only actioned 78 domains. We review all new registrations every day, routinely. I would say that for those who don't do this then perhaps there is a need to add a special rule to pull out "crisis names, like COVID" when that happens."

23," @Graeme – The 2013 RAA required ICANN to work with Registrars to identify and implement cross-field validation tools. Cross-field validation is common, automated process used worldwide; we just heard that many ccTLDs are using it to help combat COVID abuse. Will Registrars finally implement cross-field validation per the RAA? Why or why not?" Anonymous Attendee
live answered

24,"Laureen - we have talked in the RPMs PDP about the ""no fly"" concept in context of repeat cyberquatting (e.g. losing x number of URS/UDRPs), but there are challenges with how you might effectively implement this. Do you have views on how this could be done?" Susan.Payne
live answered

25,"'@David Conrad - You just wrote in chat that 8 Registries were found to be responsible for 90% of phishing. DAAR data is useless. When will DAAR tell us, for example, who the 8 registries are? Which registrars have the highest % of abuse in their portfolios? We've been asking for actionable data for years and years..." Anonymous Attendee
The 8 registries likely correspond to the 8 largest registries since the measure is based on absolute numbers.,,,

26,"So that brings me back to the initial question, were the names reviewed after the harm had already been done and the fraud done?" Fabricio Vayra
"For us, the domain would be checked at regular intervals, but just once. It's not as though it's checked once for DNS Abuse and if its OK it is not checked again."

27,"The previous panelist talked about shield approach but the wish list was restricted to what data is collected and its accuracy, why not shield users by having safeguards about who the domain name goes to? At leasrlt names such as curecovid.com (imaginary) which have a high propensity for abuse (for e.g) ?" Anonymous Attendee
live answered

28,"'@David, where you've spoken to registries regarding anomolies, is there usually a positive outcome?" "Donna Austin, Neustar "
"Yes, generally."

29,"'@David - would be good to have a DAAR report that normalizes data vs. domains in registration data, which ICANN has at least for gTLDs. Then you have a really interesting top X list to look at for registries and registrars since % of abuse is really the key issue." Rod Rasmussen
it;'s in there (if i understand what you're asking)

30, what is the accuracy percentage of DAAR? thanks, Rolla Hassan (GAC Egypt)
"I'm not sure I understand the question. DAAR collects information from DNS reputation providers, that is, it is based on reports made to reputation providers who have vetted those reports using their own processes. DAAR does not modify that data."

31,"The efforts, projects and initiatives of RrSG, OCTO and PSWG towards identification / reporting of Pandemic Related Domains are worth mentioning. More such interactions should take place in future, and experiences, best practices and case studies should be shared." Mohit Batra
Agree!

32, How are we to move forward to agree a definition of DNS abuse? As at present figures presented are very different as one assumes different criteria used. Thanks, Nigel Hickson
"Nigel, the CPH has agreed upon a definition. Use that!"

33,'@Bruce - Any chance we can hear from ICANN compliance about what they plan to do? Fabricio Vayra
"We will take this to ICANN org, thanks!"