ICANN81 | AGM – GNSO: CPH DNS Abuse Community Update
Thursday, November 14, 2024 – 13:15 to 14:30 TRT

SUE SCHULER: Hello, and welcome to the session of the CPH DNS Abuse Community Outreach. My name is Sue, and I am the participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy.

If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak. Please state your name for the record and speak at a reasonable pace. I will now hand the floor over to Dennis Tan and Reg Levy.

DENNIS TAN: Thank you, Sue. Welcome, everyone, to the CPH DNS Abuse Community Update, ICANN81. I'm here joined by Reg Levy, my colleague in the Registrar Stakeholder Group. I'm myself again, Dennis Tan, from the Registry Stakeholder Group. We're joined today. Can we go back to the agenda, I guess? There you go. So today, we're going to give you an update from the CPH as well as Leticia is joining us to give an update on ICANN Compliance as we are seven months into the DNS Abuse Amendments that were effective as of April this year.

First, we're going to hear from Graeme Bunton from the NetBeacon Institute, and he's going to give us an update on the Abuse Reporting Guide that the CPH put together and is now going through a revision just because the DNS Abuse Amendments. And then we'll follow up to a conversation with Leticia starting with an update from ICANN Compliance, followed by a Registrar and Registry's perspective regarding the DNS Abuse Amendments. Reg, do you want to say something?

REG LEVY: No. I'm looking forward to the presentation from Graeme because the Registrar Stakeholder Group has been working on a reporting guide for many years, and we're looking at updating it. Pardon me. It's been a long week, and I'm losing my voice. We're looking to update it so that it is fit for purpose for the DNS Abuse Amendments.

DENNIS TAN: Thank you, Reg. So, without further ado, Graeme, please.

GRAEME BUNTON: Thank you, Dennis. Thank you, Reg. Hello, everybody. We're so deep in this meeting. It's tough to have some energy in the room, but I know we can do it. Let's try and have a little bit of fun as we talk about DNS abuse. All right. Next slide, please. So, my name is Graeme Bunton. I'm the Executive Director of the NetBeacon Institute, which is a project from PIR that spends all its time and energy trying to reduce malicious domain names. And I've been asked to help on this project, and I'm

super happy to do so because reporting abuse is very near and dear to my heart.

The CPH has a set of guidelines that it published, I think, pre-2020 on reporting abuse. I'm pretty sure it happened when I was still a registrar. And so, it felt time in any way, because it's been a little while, to update those guidelines, and then really there's been some changes since then that have necessitated this work. The amendments, of course, are the biggest piece of that puzzle, but also the technology around abuse reporting and the requirements that registries and registrars need as abuse changes have also changed. And so, it was due for an update.

I suspect this will be faster than 20 minutes, but maybe we get some questions. So, where we've come to in our discussions about how to revise this work is really that we're going to aim for three different outputs. The first is really about how to identify what type of abuse you're reporting and who the responsible party is. And so, that will be a document.

The next piece is, okay, if it's DNS abuse and the appropriate party is registrars, and that should probably say also to registries where appropriate, what does that actually look like? What sort of concrete guidance can we give you for reporting DNS abuse to the industry?

And then the last one, the last output, is a visual guide for all of the above, and that's really a flow chart, and we'll talk about that in a minute. We'll go through each of these in a bit more detail. The goal is really to increase actionable abuse reports, to make sure that the abuse reports that registries and registrars are getting are abuse reports for

DNS abuse and things that they can do something about. Correspondingly, we also want to make sure that we route non-DNS abuse reports to the appropriate party who can take action for them.

This is still, in my experience, a real pain point for registrars, that they get an awful lot into their abuse queue that is just not for them. And registrars do not have infinite resources, and time spent on abuse that they cannot action is time away from reports that they could. And so, that's a really important piece of this work. And then we want to see if we can bring a bit more clarity to the responsibilities within the internet infrastructure stack, which harms go where and why. And that part is related to the visual guide, I think.

So, the first output is this how and where to report abuse piece. And it's really about how do you identify the type of abuse that you're looking at, how do you identify the venue for the type of abuse that you wish to report, and then how do you provide the required information for an actionable abuse report. So, that is going to be about a two-page document. It's mostly drafted. The reason it's not finished is my fault. That's going to be a recurring theme through this presentation, is that I think we were really aiming for having this work done by this meeting, and a lot of it just got stuck on my plate, so apologies to my registrar and registry friends and the rest of the community that I was unable to commit the amount of time I really intended to. So sorry, everybody.

Output 2 is about reporting DNS abuse. So, if Output 1 provides us like how and what to identify abuse and figure out where it needs to go, next is the details. Okay, we have DNS abuse. How do we report it to

registries and registrars? And this is really about what information is required for a DNS abuse report, what information is optional but helpful for a DNS abuse report. Also deeply important is what information is unhelpful or unnecessary for a DNS abuse report.

We're really trying to get people to that Goldilocks zone for DNS abuse reports where there is the required information, the information a registry or registrar would really need to take action in that case, and nothing more, so that we can really optimize that throughput of DNS abuse reporting. And the sort of output of this really does look like fields, descriptions, and a proposed order, you know, so that we can standardize to the largest extent possible what's coming in the door at registries and registrars, that most abuse reports look the same, because the more we can standardize that work, the faster everybody can respond to abuse reports. And so, that's Output 2.

And then the last output is a visual guide. It's a flowchart, truly, that sets out a series of yes or no questions that help people understand what type of abuse they're looking at and what the appropriate venue is for that type of abuse. And so, it covers a very broad array of bad things on the Internet. This flowchart has sort of been floating around at least registrars and contracted parties for a long time now.

And it's ordered by what I would consider severity of harm, so it starts from the very worst stuff that needs the most urgent action all the way down to, boy, I'm not going to tell you what it is, because maybe that's controversial and this isn't the forum for that, but harms that are not threatening human life. And so, that's the order in which these

questions are asked, and it should hopefully direct you to the right place for that particular type of harm. And this is a screenshot from the draft. We're going to make it pretty so that it's actually consumable by a normal human.

Next slide, please. Oh, that was it. So, maybe I'll stop there. And just to summarize, we're working on some new abuse reporting requirements that we will share with the community. There's three outputs in there, the how do you identify the abuse type, and where that abuse report goes, if you're reporting DNS abuse, what information is required and helpful, what information is not, and lastly a guide to help you understand where abuse reporting should go. Any questions on that work? Please.

ALEXANDRA ZINS: Sorry, I wasn't quick on the zoom. Hi, this is Alexandra Zins from Fairwinds. I recall back in Paris at the CPS meeting, there was a specific ask around phishing and a guide to gathering evidence and what kind of evidence was needed to report phishing and have that complaint be effective. Will that be included in this document as well?

GRAEME BUNTON: Yes. Thank you for the question. Yes. I will say it is really mostly focused on phishing. It is the most commonly reported harm to registries and registrars. And so, the work we see 99.9% of everything is phishing. And so, we'll try and address things like malware and botnets and spam as a vehicle, but it will be largely targeted at phishing. Great. Okay. If

anybody wants to provide some input or chat about this work, I'm happy to chat. I'm pretty easy to find and contact. If you want my card, I'm here. Otherwise, I'll pass back to you, Dennis and Reg. Thank you.

DENNIS TAN: Thank you, Graeme We look forward to reviewing that work. Thank you very much for the support and help. All right. So next we're going to jump to the next topic, The RA/RAA DNS Abuse Amendment: 6 Months on, which is actually 7, but data points on 6 months. So, I will pass on to Leticia from ICANN Compliance. She will give us an update on that. Thank you.

LETICIA CASTILLO: Thanks, Dennis. Hello, everyone. My name is Leticia Castillo. I am a senior director with ICANN Contractual Compliance here with an update on the first six months of enforcement of the new DNS abuse mitigation requirements. If you attended the session on Tuesday with the GAC or read the report that we published last week, you've seen some of this data. I will share a couple of additional details so it doesn't feel repetitive, but these are important outcomes to share.

On April 5th, 2024, the new requirements became effective. And from that date through October 5th, 2024, we initiated 192 investigations with registrars and registries that specifically included at least one type of DNS abuse, mainly phishing where the domain names were reportedly being used to try to impersonate governmental institutions, as well as other private entities such as online stores, hotel chains and

financial services entities, for example. Most of these cases were reported by information security researchers followed by representatives of the entities being impersonated, sometimes employees and sometimes attorneys representing the entities.

Two of those investigations resulted in formal notices of breach, one to a registrar, one to registry operator, and 154 DNS abuse investigations were resolved within the informal resolution stage of our process, which is the stage where most investigations are resolved enclosed across all competing types, not just abuse, because the contractor party either demonstrates compliance or takes actions to remediate a non-compliance before escalated compliance actions are taken.

One single investigation can involve one domain name or multiples and one investigation into a number of domain names can result in the discovery of additional abusive domain names that are also act upon. And this is why 154 investigations resulted in the suspension of over 2,700 domain names and the disabling of over 350 websites in this case because the registrar or its reseller was also acting as a web hosting provider.

Important to know that this are the numbers for the first six months. We have a lot of cases going on. We have a lot of cases that were closed after October 5th. So, the total number will be provided in future updates. But I took a look at the numbers last night. For example, from October 6th through November 12th, we initiated 38 new investigations and we resolved 32 more.

During the first six months, we participated in multiple outreach events related to the year requirements like in-person workshops with contracted parties in Beijing in September and here in Istanbul in October where there was a lot of discussions related to the DNS abuse requirements. We participate as much as possible in this type of capacity building initiatives that are mainly led by our GDS and GSE colleagues. And it's important to us to reach out to the community and not only provide our data but also participate in discussions about the requirements and explain the requirements and help those contracted parties that need it to become compliant and stay compliant.

In June, we began publishing our new monthly updates related to the enforcement of the DNS abuse requirements. These reports are broken out by the type of DNS abuse. They begin with data from April 2024 and they are updated every month. We understood that this format that we use while complemented with regular updates like the one that we provided last week with the report that includes examples and more context could help provide a comprehensive picture of all the enforcement actions we're taking and what we're seeing. But we designed this report as a starting point. The intention has always been to continue building on them and improving them over time and we welcome feedback from the community to do so.

We actually published a blog back in June when we launched the report that explains how that feedback can be provided to us. If any of my colleagues here can post a blog in the chat, that will be helpful. Lastly, we just launched an audit to validate compliance with the registry agreement that includes but is not limited to DNS abuse requirements.

And as I mentioned before, on last week, on November 8th, we published a detailed report on the first six months of enforcement. My colleagues can post the link in the chat as well and it's on the slide.

Next slide, please. This chart summarizes the reasons for resolving the 151 cases that I was mentioning before, 151 with registrars, next one is going to be the three with the registries, with respect to DNS abuse investigations. In approximately 52% of the cases resolved, the registrar confirmed the DNS abuse, suspended all the domain names involved. In approximately 21% of the cases, the registrar did not find actionable evidence of the DNS abuse and the response was deemed compliant because it included a reasonable explanation of the investigation that was conducted and how the conclusion was reached.

For example, a registrar reviewed all the information they had regarding the report, regarding the domain name, including account information, communications with the registrants and determined that the registrant had been approved by the entity that was believed to be impersonated to conduct a simulated phishing program for which the domain name was being used. That's one of the examples.

In approximately 12% of the cases, the registrar took other action to stop the use of the domain name for DNS abuse, for example, by sinkholing the name service so that users trying to reach the malicious domain names were redirected to a different IP that was controlled by the registrar. I believe I missed the other 12%, just in case. In approximately 12% of the cases, the registrar took action to disrupt the course of the DNS abuse, for example, by forwarding the claim to the

registrant and then took action to remove the URL where the DNS abuse was placed. This is for registrars.

If we please move to the next slide. This is information about the cases resolved with registries. We resolved three. All domain names were suspended. Again, just resolved. We had others going on and they were initiated afterwards. We had a fourth case that was limited to the two issues with the abuse contact displayed and those were resolved in the case close as well. Just to point out the difference between the number of cases resolved with registrars and resolved with registries is consistent with the fact that of the total number of complaints we received, 94% referred to registrars and of the investigations that we initiated, 97% referred to registrars.

But there's no minimum required for us to start an investigation or to escalate an investigation. Proof of that is that during the same time period, we issued a breach to a registrar and a registry. We intend to continue publishing our monthly reports and our regular reports and participate in these discussions and outreach to the community, so stay tuned. And I'm happy to take any questions.

DENNIS TAN: Thank you, Leticia, for that update. I think we have time for a few questions here. Jeff?

JEFF NEUMAN: Yeah, thanks. This is Jeff Neuman. It's more of a comment than a question. I think it's great to see the results of ICANN's enforcement. I

think this slide somehow, it kind of leaves the impression that DNS abuse is only acted upon after ICANN Compliance gets involved, and I know that's not what you're saying. I just want to make the point that you know, tens of thousands, if not more than that, of domains are taken down by registries and registrars without the need to ever involve Compliance. So, I think it's an important point to make that although we're having Compliance come and present, the bulk of the names that are taken down every month don't even see Compliance at all. Thanks.

LETICIA CASTILLO: Thanks, Jeff. Absolutely. This is just an update of the cases that Compliance get to see. We don't have visibility over the entire DNS market or all the actions that registrars, registry and other actors within the DNS ecosystem take to address abuse, DNS abuse. Thanks, Jeff.

DENNIS TAN: Thank you. I think we have time for one more question for the ICANN updates. Looking through the room. Okay. I see no hands. Oh, I see one hand. Mark.

MARK DATYSGELD: Thank you so much. Mark Datysgeld. Thank you for the presentation, Leticia. You were majorly important during the DNS abuse negotiations, so thank you for all the help then as well. One matter that is a point that is not quite clear, I was reading through the report, is about timing. One of the key aspects during the DNS abuse negotiations was providing you and your team with the correct

resources and tools necessary to take swift action. We settled on something like that. Not immediate, but swift. What do you feel about the time of resolution that these complaints are having? Is it a long lead, a shorter lead, and is there anything else that would be helpful for you? Thank you.

LETICIA CASTILLO: Thanks, Mark. So, in terms of timing, I see two different types of timings. The timing that takes for an investigation to be completed. It happens that we get the case forward to the contracted party. The domain name may be acted immediately after receiving our case, but we detect a pattern that indicates that the process was not in place to address the DNS abuse without Compliance being involved.

So, even though the domain name has been acted upon at that moment, the case may last weeks or months while the contracted party put a process in place to ensure that they act on the DNS abuse without us ever contacting them. So, we get the process, we get the description of the process, milestones, timelines, and then we wait until those are implemented, confirm they're implemented, close and monitor. So, the case can take long, even though the specific domain name has been acted upon.

When it comes to the timing for mitigation itself, this was discussed in length back in the negotiations and afterwards, but what's prompted highly depends on the context, but we have seen several cases where the example I was saying before, we send the case, the domain name is acted upon immediately, immediately after receiving our case, but not

considering the time that the registrar or the registry had from the moment they were notified of this.

So, it could happen that actual evidence was not obtained until recently. It could be a coincidence so that it's reasonable and we will take that into account. It could happen that the investigation did not really start until we contacted them and that is not acceptable, so that would require a remediation plan that we will monitor as well. So, it depends on the case, but timing is for sure something that we take into account because the longer an abusive domain name is allowed to continue to perpetrate abuse, the more harm it can cause.

MARK DATYSGELD: Thank you very much.

DENNIS TAN: Thank you for that question, Mark. Anyone else? All right, I see no one, no hands. Okay. So, we move on to the next part of this section. I will turn it to Reg to give the registrar perspective on the six months of the amendments.

REG LEVY: Thanks, Dennis, and thank you, Leticia, for the update from ICANN. From a registry perspective, we have seen an increase in complaints about DNS abuse. We've also seen an increase in complaints about not DNS abuse but classified as DNS abuse. Closer to the mic, sorry. And

we have not necessarily yet seen an increase in valuable actionable reports. So, we are pleased that these amendments were passed.

We took those as part of the drafting team, but we are looking forward to the community also improving the types of complaints that they send to us and the quality of the evidence that they provide to us. We're also seeing an increase in complaints going to ICANN about domains that were reported to us for abuse. So, at least the community does know that ICANN has the ability to enforce these amendments, and that's a very positive step in our imagination.

DENNIS TAN: Thank you, Reg. We have time, so I've just maybe one other registrar wants to share their perspective, but completely voluntary. I don't want to put anyone on the spot. All right. So, from a registry standpoint, and this is Dennis Tan for the record, we see the same thing. We don't get the volume of abuse reports that a registrar might get, but the ones that we are receiving, it varies, but we've seen some increase in the quality of reports, and obviously that's what we want. So, I think that's the positive side on the amendments, raising the quality of the information that we get so that we can do something with it.

But that's in the past, and so I just want to take this opportunity to also say something about what's in front of us. We've seen, I think, many of us in the community were expecting the infirmary report. It's now published. People are consuming that interesting report, and we look forward to continue this conversation, DNS abuse evolving the implementation and what we can do as a community to start working

on solving the problem. Whether that's a PDP or something else, as a CPH, we are open to those conversations and to continue that work. So, yeah, I think that's what I wanted to say.

I think we're going to end early, so you guys can get out of here and go visit the city or do something fun. So, I think that's for our agenda, right? Can we go back to the agenda? Oh, yeah, it's Q&A. Okay. So, now it's Q&A for everything. So, it could be for the agenda or anything else that comes to your mind related to DNS abuse, of course. Okay. I'm just going through the room. See any hands? I don't see any queue here on the Zoom.

So, I think that's it. And please enjoy the time back on your day, and thank you very much for joining us today. We look forward to seeing you back in Seattle, and we probably will have more information to share with you. The complete abuse reporting guy, for sure. And that's it. Have a good rest of the day. Thank you.

SUE SCHULER: We can end the recording.

[END OF TRANSCRIPTION]