ICANN82 | CF – GNSO: CPH DNS Abuse Community Update
Sunday, March 09, 2025 – 15:00 to 16:00 PST

SUE SCHULER

Hello and welcome to the CPHD DNS Abuse Community Update. My name is Sue and I'm 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, onsite 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 Reg Levy.

REG LEVY

Thank you. Next two slides, please. Thank you everyone who is joining us today. Thank you especially to non-contracted party house members. This is the contracted party house DNS Abuse community update. We are here for you.

The agenda's on the board above. I will shut up very quickly and then turn it over to Graeme Bunton, who is the executive director of NetBeacon who will be presenting a number of documents that the CPH has been working with NetBeacon on for some time in an

attempt to have better reports so that reporters can get things to us in a manner that will allow us to action them faster.

Then we're going to discuss additional community work and turn it over to a Q&A, and we hope that there will be robust debate and questions from you all. My name is Reg Levy, I should have started with this. I work at Tucows and with Luke.

I am the co-chair of the Registrar Stakeholder Group, DNS Abuse Subgroup, and together with Dennis and Chris, who are the registry sub chairs for DNS Abuse, their subgroup, we are the joint four group chairs for the CPH DNS Abuse subgroup. And with that, I'll turn it over to Graeme.

GRAEME BUNTON Thank you. Hey, everybody. My name's Graeme Bunton, I'm the Executive Director of the NetBeacon Institute. Really a part of Public Interest Registry which allows us to hang out with the CPH. And the fun bit about our jobs is that we get to try and make the internet safer all day. And sometimes that means producing resources for the CPH. So thank you. I'll slow down. I appreciate that.

Next slide, please. So a long time ago, pre 2020, we had, as the CPH developed abuse reporting best practice document. And it was just overdue for an update. Things have changed. The amendments have come into effect, the technology has changed, requirements have changed, so it felt like the time was right to begin updating and revising these documents. And so we have put out there, I

think they're online and publicly available at this point. Thank you, Zoe.

We've updated that guidance for the community. I will put this out there though, which is that probably we should be updating these things more often than every six years. They're not policy documents. They're not binding in any way, what we're trying to do is provide resources that are helpful for the community. And so what I think we should sort of approach these like in the future, is more of a living document. And so we would love feedback, we will try and update these more frequently, keep them fresher than once every five years.

So please, as you're looking at these resources, don't see them as like stamped in stone. You know, they may not be perfect, in fact, I'm sure they're not. Please engage with us in conversation, tell us what works, what doesn't, we'll tell you what works, what doesn't, that's part of this session here today, and we can continue revising these resources for everybody.

Next slide, please. Right, so this work, and this is gonna be a gentle rehash of some of the update I gave in Istanbul. We have three resources now. One is an abuse reporting guide that starts from a pretty wide funnel. It's really trying to help people identify what type of abuse they're looking at, and then who that responsible party might be. And the goal there is really to increase the actual abuse reports trying to route non-DNS abuse to the appropriate party, not the registrar or registry, and help bring some clarity to these discussions.

We have another document, which is an effective DNS abuse report, which is really, in many ways it's a spec, it's a set of fields, some required, some optional for reporting abuse to a registrar to really help specify, like, make super crystal clear, this is the information that is required in order for an abuse report to be successful.

And then the last thing that we produced that I think is quite interesting and fun is an sort of online harm flow chart. We wanted to help people understand where in the stack DNS abuse gets reported and where to go for other online harms. And so it's a visual guide to help people sort through what sort of problem they've got and where they should begin reporting it. And we're gonna look at these resources shortly.

Next slide. Like Graeme says. Okay, I don't need to read that. So this is the first document I was talking about, helps you identify that type of abuse report, helps you figure out the best venue for that abuse report, and provides the required information for an actionable abuse report.

And there's a link there that's up and it's live. And where did the slides go? Oh, we're gonna actually look at the document. How about them Apples? Thank you, Zoe. I don't know that we need to collectively go through all of this at this point.

I think everybody can get the link from the Zoom. Can we dump the links into Zoom? They're in there already. Bless you. People are better than me at everything. So this is that first document that's really talking about different types of abuse and where you

can go. And I think that's-- I don't know that we need to go through this in more detail. It gives you steps, it gives you ideas, it gives you references to tools like Acid and NetBeacon Reporter. And there you go. Oh yeah, big note on CSA there. Do not send that to the registrar or registry. Send that to your local in hope provider or CCM Authority.

All right, next slide please. Right, this is the spec. This one we can maybe look at in a little bit more detail because I think this detail is helpful here. So what we did is we went and looked at what an effective abuse report contains and tried to turn that into a really concrete list of fields. And so this document that I think we can bring up, please and thank you, proposes what an email subject for look should look like if abuse is being reported via email instead of web form.

So we've got examples there. It should be the type of harm, the domain name in question, and who's reporting it. And so we have two examples. And then we talk about the order of the fields. And this is really about optimizing registrar abuse practices so that they're getting the information that's most important for them, that they need to take action as early as possible in the report.

So this is the information ordering. We talk about the abuse itself, if there's any extra information about the domain name, if there's any information about who is reporting the abuse, and lastly, any information about the evidence or attachments included in that report. Keep scrolling, please.

So we can go through these first piece. I don't know that we need to go through all of it but we want the defang domain name and the URL and the abuse type, a brief description of the issue. Reg and I have had some fun conversations about this. She wants like two words, I think probably no more than two or three sentences.

If the abuse requires more description than that, then probably there's a problem. We really want to know the targeted entity. This is really important if it's phishing, especially, we see now lots of crypto related phishing, and the entity being targeted is often unknown to a registrar or if it's a different jurisdiction, different language. You can't expect a registrar to know who the authoritative domain name website really is.

If it's a bank from somewhere else, I might not know that bank. And so, including who is being targeted and their official website can be really important for reports of phishing. We want to know when it was last observed so that that abuse report is fresh. And then verification requirements is also increasingly important as we see increases in what's called geofencing, making it really hard for registrars to verify abuse.

So if this abuse is only visible on a mobile phone, on a particular network or in a particular geography, we want to be able to provide that to a registrar so they can try and verify and replicate the abuse. And those are the key bits for an abuse report that we really want to make sure we have. There is extra information that can be included in here, and I think all the rest of the fields, aside from the evidence are optional.

Can we scroll down a bit? DNS records name servers, days since registration is often super helpful. You know, if the domains existed for two days, the potential consequences for suspension are lower. Keep scrolling down. Thank you, Zoe.

A little bit of information about who's reporting it. And then lastly, the evidence pieces. Screenshots are still key within the industry. Everybody would really like screenshots in order to understand what abuse is happening, especially if it's related to phishing. We want to see in those screenshots evidence of impersonation, and we want to see evidence of attempting to capture sensitive information. And without those two pieces in the screenshot, it's really hard to make a definitive choice. And so please include that, and you really have to for an effective abuse report.

We've talked about this a little bit in the past, reporting only abuse that's only in an email, there's no resolvable website, is really difficult for registrars to action without email headers and bodies. And I understand that those are complicated to get and hard and it's really difficult to train people how to get those. You cannot do it in your most email clients on your mobile phone anymore. This is an interesting topic for more discussion, but generally, for registries and registrars, they're going to require those in order to take action for email only abuse.

And so that is the second document, the spec for reporting abuse. We have some examples in there. Don't mind my Canadian socialist commentary about banks of capitalist exploitation.

Mostly my own jokes. But that's what an effective abuse report is. It's that long.

Sorry, can you scroll back up? This is a minimal abuse report. It doesn't need to be longer than that. In many circumstances, it should absolutely not be longer than that. This is what a registrar would need to take action. And then we have another example with more fields. Sometimes that more information is helpful, not always. Cool. Thank you. What's that? We have a hand raised. Oh, please.

MARK DATYSGELD: Mark Datysgeld, BC. Graeme, could you clarify a bit the concept of geofencing? Dive a little deeper into that, or somebody who has deeper understanding.

GRAEME BUNTON: Great, thank you. Helpful point, Mark. So geofencing is a technology a method that bad actors use to prevent other people from seeing, let's call it a phishing website, because it's most commonly a phishing website. It prevents other people that they don't want to see that phishing website from accessing it. So when you get an abuse report as a registrar for a Canadian bank, say, or the Canadian Postal Services, another pretty common one, we'll see, and it's only visible on your mobile phone on a Canadian telco.

And so they've implemented technology on that website that would only let someone with those attributes see it. And if you're coming from outside, say, the domain is registered with an

American registrar and they're in Seattle and they want to go verify this abuse report, but it has that blocking in place, they can't see it, they can't resolve that website. Maybe they get a 404, maybe they get a CloudFlare blocking page, there's lots of different ways that people implement it, but it presents a real challenge for registrars. So including some of that replication, that verification information is helpful. Any other questions on this one? Cool. And there's I think a 20-minute Q&A at the end of this, and so if something comes up in your brain as we move on, feel free.

Let's keep going. Flow chart. This is a fun one. Yeah. So this is a pretty high level view of how we saw abuse reporting working. And we ordered this flow chart roughly in terms of severity in urgency of harm. I'm sure we could quibble with the order that we put things in, but I think it's largely correct, directionally correct. And what it's really trying to do is direct people to the right place for particular harms. Are we able to pull up the actual thing? Thank you, Zoe.

REG LEVY I've also dropped it into the chat if you want to follow along at home.

GRAEME BUNTON Oh, and that's probably better because It's long. It's pretty hard to make all these choices fit on a single screen. They're working. Boy, it's really weird staring at yourself like that. Okay. How to report online arms in a relatively simple flow chart.

Again, ordered roughly by severity of harm, so we're trying to make sure that the most urgent thing, which we think of as the most important information like, oh God, help us if someone's in an emergency situation referring to this. But that if there's an immediate, incredible threat to human safety, please go contact law enforcement.

Is there a report of CSAM? Contact your local CSAM authority, NICMIC, IWF, In Hope Network, do that. Is there an issue related to human trafficking, distribution of opioids, or a credible threat to safety? These are issues that were highlighted in the framework to address abuse that many contracted parties have signed on to, and so you should A, contact law enforcement, and then B, you can contact the web host, and CC, also the registrar if they're a member or a signatory to the framework.

The next box is the one we're sort of here to address. The purple boxes is, and I don't know why it's purple, interesting choice, designer, is DNS abuse. And this is where we're seeing issues related to phishing, botnets, malware, farming, and or spam as a vehicle for those, contact the web host and the registrar. We at the NetBeacon Institute, we'd love to help you do that. Please come talk to me.

Next down, is the issue related to content on a platform like Facebook or Reddit? You should go to the platform. Is the issue with the domain name, is it trademark related, you should contact the registrant, is it cybersquatting, again, the registrant, URS UDRP to escalate that. Is the issue related to content on a website? You

know, your first stop is the website administrator. Do you go deeper than that? Do you contact the domain registrant? If you go deeper than that, you contact the web host.

And lastly, if it's related to some other service, email, FTP something else, you should be contacting the particular service provider for that, which might be an email service provider, it might be a host, it might be other.

And so hopefully that is a helpful guide for people to understand where to report different types of things that they're seeing online. And I think that is the extent of our slides and work here. Happy to take questions or people can hold that to the end. Thank you to everybody in the CPH who contributed to that work. And just to reiterate, I don't think any of us think this is perfect. We would love more feedback and input to keep refining these documents over time. Thank you.

REG LEVY: Thank you, Graeme. Next slide, please. This is a discussion or quick synopsis of some of the cross community work. Yeah, that's some of the work that we've been doing within the ICANN sphere. Next slide. Thank you. And I'm gonna turn over to Dennis to address the SSAC one.

DENNIS TAN: Thank you, Reg. Dennis Tan, Verisign, here. As part of the CPH outreach, we met with a few groups here. So these are the list I'm gonna touch on the topics that we talk about with the SSAC and

follow up on work. During our discussion, just different topics came up, and these four, so the use of artificial intelligence or how Reg would like to refer to as large language models.

Is that correct? Yes. For the use of DNS abuse. And I think many anecdotally or not, you have read about these phishing kits getting more sophisticated with the use of these tools. It was a presentation that SSAC did in Istanbul, so we wanted just to get additional insights and feedback from that.

Then we discussed some insights about the INFERMAL report. I think most of you maybe already know, but this is a study on a malicious registration done by the ICANN OCTO office. It was published last November, and there have been a subsequent webinar on that report and the conclusion.

So I encourage you to read the report and watch the recording of that webinar. If you have not, very insightful information. Again, the INFERMAL report, it's a study of a point in time and study of what many of us know, anecdotally of what happens with malicious registration, which just give more data with good methodology and whatnot. But the findings not really need to be taken to and used to jump to conclusions.

It's information for us to look at next steps. The other two, the last two, the other field for DNS abuse and one-on-one guidance, more on the technical operational things. The other field refers to a RDDS flag or a set of data that the RDAP protocol can return to

signal some feedback to reporters in terms of what have been happening on domain name and that had been reported for abuse.

And that's actually a topic that was discussed this morning during the CPH Tech Ops session number one. So if you are interested in that discussion, watch the recording of that report, sorry, the recording of that session.

So it's something that the CPH Tech Ops is keen to take on, and so we'll hear more about that in the future meetings. And regarding one-on-one guidance, and I'll tend to Luke in a minute because I think that's something that Luke wanted to discuss.

This also was brought, it refers to a little bit more on the reporting as well. So when you have more technical issues and reporting like email headers or a basic checklist for reporters to check on the domain name status and domain name settings before they issue a report. And I think the use case was a report on email issues when the DNS records don't have any mail records, something along those lines.

So Luke, do you want to add something to that? No. Okay. So that's good. So that's the extent of the meeting with SSAC. Again, the one thing that is active right now is the field for DNS abuse. So that's something that the CPH Tech Ops has taken and is gonna progress in future meetings, so we'll report back when we have more information. Back to you, Reg.

REG LEVY

Thank you, Dennis. And with regard to the one-on-one guidance, we say things a lot like I need the email headers. And for a lot of people that means the two field, the subject field, and maybe a carbon copy field. So describing these things better for your average internet user is absolutely something we could be better at.

Luke dropped into the chat an explanation of, for example, how to find those headers, which we are going to work on being better about doing. With regard to engagement with the NCSG, they have an ongoing desire to explore human rights impact assessments with regard to DNS abuse.

What are the consequences to a legitimate registrant for suspending a domain that might have been compromised or that might be seen to be doing something that it isn't doing or reported for doing something that it isn't actually doing?

So yesterday, as everybody knows, the meeting starts tomorrow, so we went back in time. Yesterday we had a session where we were given information by the NCSG about what a human rights impact assessment is and how to conduct one, including a list of questions that can be helpful in terms of going through your choices identifying the human rights impact at each stage of your process of evaluating DNS abuse.

And then we also had breakout sessions. We love a breakout session. And we examined and discussed specific case studies in groups. There was also a really fascinating example that was shared by an NCSG member from, I believe, Sudan, about an issue

where a number of domains had gone dark and there was a suspicion that it had been government action, but it wasn't. It was some sort of DNS abuse and all of the fallout that occurred from that.

So it has yet to be resolved, but really interesting impact examples of what happens when we get it wrong. With regard to the CSG, if you guys wait, here in this room, after this session, we'll be presenting along with the CSG about DNS abuse report examples that they are finding difficulty getting the abuse mitigated and examples from the contracted parties of reported as DNS abuse, but not actionable as DNS abuse.

Next slide, please. Excellent. Has anyone any questions or possibly, answers? I could use some answers. Did I see a hand? No. Tough crowd. All right. Well, we are here. I'm going to give it a couple more moments, otherwise I will give you back some time in your day. All right, I know we did great. We explained everything, no questions at all. Love it. All right, thank you, everyone, and have a great day. We can end the recording.

[END OF TRANSCRIPTION]