ICANN74 | Policy Forum – GNSO: CPH DNS Abuse Community Outreach
Wednesday, June 15, 2022 – 16:30 to 17:30 AMS

SUE SCHULER: Thank you. Hello, and welcome to the CPH DNS Abuse Outreach session. Please note that the session is being recorded and is governed by the ICANN Expected Standards of Behavior. During this session, questions or comments submitted in chat by participants will be read aloud if put in the proper form as noted in the chat.

Taking part via audio, if you are remote, please wait until you are called upon and unmute your Zoom microphone. For those of you in the auditorium, please raise your hand in the Zoom Room, and when called upon, go to the standing microphone in the front. For the benefit of other participants, please state your name for the record and speak at a reasonable pace. You may access all available features for this session in the Zoom toolbar. And with that, I will hand the floor over to Brian Cimbolic.

REG LEVY: This is Brian Cimbolic. This is Reg Levy from Tucows. I'm co-chair of the Registrar DNS Abuse Subgroup. I would like to welcome you all to The Hague and to our wonderful outreach session on DNS Abuse. May I have the next the next slide and then the next slide after that, please?

This is a brief agenda for our time here today. So I'd like to put these questions on the screen just for you to think about while we are introducing some of our speakers for today. We'd really like your input

about what it is that we can do to help various initiatives around the community on DNS abuse. And I'm now going to hand it to Brian to explain what DNS abuse is.

BRIAN CIMBOLIC: Thank you, Reg. Next slide, please. Hi, everyone. I'm Brian Cimbolic, I'm at Public Interest Registry. So as we're having these discussions, it's important to keep in mind this is the CPH session, and the CPH has published a working definition on DNS abuse.

This is probably no surprise to many of you but the CPH defines DNS abuse as malware, botnets, phishing, pharming, and spam when it's a delivery mechanism for one of those prior forms of abuse. So, just as we're having these conversations, when you hear us reference DNS abuse, I know there's varying definitions of DNS abuse in the community. This is what we're talking about from a CPH perspective. And with that, I am happy to introduce the sort of guest speaker to our CPH Abuse sessions. Samaneh from OCTO is here to talk about the four-year DNS abuse retrospective. So with that, I will hand things over to Samaneh.

SAMANEH TAJALIZADEHKHOOB: Thank you, Brian. Hi, everybody. I'm Samaneh, director of Security Research, SSR Research from Office of CTO at ICANN. I'm sure most of you heard about the Domain Abuse Activity Reporting Tool. The few slides I prepared today is not specifically about the tool but mostly the data that is used outside of the tool to basically explore the trends that we have seen in the past four years. Next slide, please.

So just a glance at how the tool works. It basically takes the domains in the zone files and domains in the reputation block lists as inputs, collapse those and creates TLD security threat metrics. Those metrics are absolute counts of the number of domains that are listed on this reputation list as well as normalized scores or metrics, if you wish.

The output of the system is daily scores that are accessible via ICANN, most API for registries who are participating which are gTLDs and volunteer ccTLDs, also monthly reports that in case of gTLDs, it's public, and for ccTLDs, it's tailor-made and personally e-mailed to them. Now, what we did recently is that we took the data out of the system from the first time that the system has collected data which was October 2017, and simply looked/explored what we see in the data overall. Next slide, please.

So this is how the domains in the zone files grew. This is very expected in October 2017. We saw about 185 million domains. We had around 1200 TLDs. Today, the last data we had from May 2022, we see around 207 million domains and around 1180 TLDs. Next slide, please.

Just mind that this presentation today only includes the gTLD since the ccTLD data is not public. When we look at how the security threat domains are distributed over time, this is the trend we see. We categorized the data into legacy gTLDs and new gTLDs, similar to what you see in the DAAR reports. What was kind of significant in this window of data when we look is that from 2017, we see reduction in the total number of security threat domains that are listed.

We have details of percentages. This is important because from our input data, around 92% of the data is spam as delivery mechanism,

and 3% or less for the other types for which we collect data. That is phishing, malware, and botnet command and control. That is way less in May 2020. What we suspect, again, these are just speculation, is that we have to have in mind that from 2017 to 2022, a lot of things have changed. Detection is harder than before due to GDPR and the vertical line you've seen the plot is where GDPR went to effect. So detection has been harder. The reputation block lists became more accurate, therefore, less false positives, also simply changing the trend as the data reports. We also see that the proportions shifted a bit. So in 2017, 92% of the data was spam, and in 2020, the proportion is less to spam, more to phishing and other types. Next slide, please.

Because the biggest part of this data is basically spam as a delivery mechanism, we also created visuals in which we excluded spam to see how the trend looks like. In this plot, what you see is that trend where spam is excluded from the data for the total count of security threat domains. So if we compare to 2017, today we still have slightly less security threats. But again, the difference is way less than when spam is included. So, one can conclude that the big change that we see in the overall threat domain actually happened mainly in spam, volumes and values. Next slide, please.

Then we also calculate a score or a normalized metric, which is just a sum of all the domains that are listed as security threat over the total sum of the zone file as a percentage. If you look at how that trend looks like—next slide, please—then here we see a big difference between the new and legacy gTLDs. We see lots of ups and downs for the new space, which is expectedly so, whereas the legacy gTLD space

has less variation. And as of today, we see that in total together, they form less than 1% of the overall domains resulting in the zone files.

We have the similar plot again, if I'm not mistaken, in the next slide, where we excluded spam again. So looking at this, you see that the new gTLD space has been influenced much more in the other threat types, that is phishing, botnet C&C, and malware, whereas the legacy space has been more stable. If you note the Y axis, here you see that the percentage has changed a lot. So there we had maybe less than 1%, as total on here is around point 0.1% of the old data. Also another indication that spam is a big, big portion of the data. But that doesn't change the trend a lot more. Next slide, please.

I think this is the final slide. This also shows how separate types evolved over time as a percentage. As you see, the trends for phishing and malware are quite comparable. But command and control had shifts when GDPR went into effect. Spam has decreased a lot over time, the values and volumes. With that, I conclude the presentation and I hand over to Brian. Thank you, Brian.

BRIAN CIMBOLIC: Thank you very much. Actually, I think we are going to our next speakers, Graeme, I believe. Great.

GRAEME BUNTON: Me? No. Oh, right. Sorry. It is impossible to hear anything up here. Right. So this is work that the CPH DNS Abuse Group began following the plenary we ran at ICANN73. For those of you who weren't there, don't remember, there was a plenary that was a lot of fun, I think. It

went very well on this topic of malicious registrations versus compromised domain names. In that plenary, where we got to was generally an understanding that that distinction is important, and that abuse mitigation processes should be different for these two different types of harms.

So we've been working on a paper that sort of discusses this distinction a bit more, and then elaborates the options for mitigating each type. Well, it's not a best practice. It's really meant to be a sort of informational discussion paper. We've spent a bunch of time amongst ourselves as contracted parties sort of discussing through the various scenarios and options, and beginning to put some words on paper. We also wanted to invite some members of the security community to contribute to this work as well to ensure that we're really capturing all the information we needed to. So this work is underway, it's been stalled for a little bit. So we're really hoping to get back on track and have this paper out just ahead of ICANN75 in Kuala Lumpur. So, as a community, please stay tuned. We're hoping that moves that conversation down the road a little bit. Thank you.

BRIAN CIMBOLIC: Thank you, Graeme. And by the way, whoever sticks the sound on the spot, we can hear it much better now. Thank you. Next up is Reg. Going back to Reg to talk about the Registrar Stakeholder Group's Abuse Tool.

REG LEVY: Thanks, Brian. The Registrar Stakeholder Group created this tool following a series of outreach meetings where we brainstormed the ways that we tackle abuse and realized that WHOIS queries are very common. And everyone knows how to do them so everybody does them. That's why registrars end up with abuse reports that they can't necessarily deal with. So we created a tool that will allow you to find out who the hosting company is and what the mail server information says the e-mail hosting company might be, so that when you have an issue, you can go directly to the right place in the first instance. The screenshot up on the board, it will be also in the slides that are distributed later because I know it's a bit small of an example of what the output looks like.

So we paid for and created this tool. It is abusetool.org. I should have started with that so that I can say it at least seven times during this presentation, because apparently, that's the magic number that I have learned from advertisements. Abusetool.org is where you can find it. It's broader than DNS abuse. So this is for things that the registrar might not be able to deal directly with, specifically hosting content kind of stuff and e-mail-related concerns that aren't phishing and spam. Now I'm going to hand it back to abusetool.org Brian.

BRIAN CIMBOLIC: Thank you. I've been I've been called worse. Thank you, Reg. Actually, I will hand things over to Alan Woods to speak about some work on Spec 11 (3)(b) reporting.

ALAN WOODS: Thanks very much, Brian. Alan Woods for the update. I'm one of the co-chairs of the Registry Stakeholder Group DNS Abuse Group. I'm going to give a brief update on another paper or a piece that we are undertaking relating to Spec 11 (3)(b) reporting. So, as you will be aware, the current Registry Agreement has the Public Interest Commitment to Spec 11 (3)(b), and it's about statistical and technical analysis of the zone and reporting around that.

Now, in the past there have been a few endeavors to try and just kind of get a dig a bit more into that. One of them was the security framework, which again, just went through, provided some guidance to the contracted parties and those looking at Spec 11 (3)(b), but there was never a kind of an area of reporting. So what we have done, and it was in concert, actually, with a request from ICANN themselves. They said, "Hey, it would be great to get some reporting, some statistics coming out of the Spec 11 (3)(b). So we said from a very voluntary point of view that we would love to sit down and define how can we share those statistics transparently and openly with ICANN. And that's in effect what it is.

We have created—actually it started to be a few pages and now it's down to kind of like more of a simple one-page document because it is a simple ask. We have now shared that document with ICANN and we're just going to work through it with them and maybe tweak a bit of the language, define what are the data elements, how we would send them on to ICANN. So our aim is to have this completed really quickly. As I said, it seems to be a simple ask, it will be wholly voluntary. And our hope is to have it published and perhaps even

implemented by Kuala Lumpur. So we'll be able to watch the space, give those updates as soon as possible. Thank you.

BRIAN CIMBOLIC: Thanks very much, Alan. I will hand things back over to Graeme Bunton to talk about NetBeacon. Graeme?

GRAEME BUNTON: Thank you. Boy, I feel like I've been doing a bit of a song and dance this week talking about NetBeacon. Apologies to anybody who's heard it three or four times. Yeah, I'm seeing a little bit of nodding there. But you're not going to get the whole slide deck. You're just getting the real condensed version for this particular moment.

So the DNS Abuse Institute, with the support of PIR and CleanDNS, launched a service that we call NetBeacon last week. It is a centralized abuse reporting service. So it's a website that allows anybody to report DNS abuse through pretty easy-to-use forms and it routes it to the appropriate registrar. In some ways, it's akin to what Reg was discussing with the Abuse Reporting Tool. But we're of the mindset that for most end users, even having to know what a host is or a registrar is probably a bridge too far, and so we're trying to make that process even simpler.

It takes abuse reports from anybody. It standardizes them into a particular format so that registries and registrars are getting structured reports that are similar and reliable. We're enriching those abuse reports with useful information. And so we take the reported domain name or URL and check it against sources for domain

intelligence and append that information into the abuse report, and then we deliver it automatically. So it's live. It's working. It's delivering abuse reports to registrars right now. I know we've taken some domain names off. We registrars have gotten this information and taken some bad domain names off the Internet, which is very exciting.

There's a long list of things that we want this tool to do, ultimately. Right now it's only working for gTLDs. We need to integrate ccTLDs, and then ultimately hosting CDNs e-mail service providers. We need to add other harms. And all of that will allow us to ensure that abuse reports go to the right place for things like, say, a compromised website rather than a malicious registration where the first port of call should be the host and not the registrar, that we can route abuse reports to the right place, and then perhaps escalate to the registrar, if appropriate. We want to do some work on reporter reputation as well.

So it's live, as I said. If you're interested in reporting abuse, you can go to app.netbeacon.org or just netbeacon.org to learn some more, and feel free to give it a try. We are very interested from registries and registrars on what information they find useful in abuse reports. If there's services that they use for investigations, we would love to understand more about them so that we can include that information in the abuse reports that we sent. If you are engaged in trying to disrupt or mitigate and report DNS abuse and you'd like to talk to us about how to integrate with the tool, we're interested in that as well. It does have APIs for both ingress and consumption so that this whole thing can be used for combating abuse at the scale of the Internet. So we're very excited about this launch. We hope that you'll all check it

out. I'm sure we'll be sharing more about how it's working in future meetings. Thank you.

BRIAN CIMBOLIC: Great. Thank you, Graeme. Last but not least, I'm going to hand things over to Keith Drazek, who is going to walk us through some Q&A that we prepared but also just engage in open dialogue. Keith?

KEITH DRAZEK: Okay. Thanks very much, Brian. Hi, everybody. It's Keith Drazek, I'm with Verisign, and I'm here to facilitate the Q&A. So we've got some questions that we've teed up but you're not limited to these questions. If you have anything else that you'd like to raise with the folks here, we'd be happy to take them.

So the first question for the community that we've come up with is, what initiatives are the SG and ACs engaging in outside of CPH, for example, hosting providers, e-mail providers, and CDNs, is their scope for the contracted parties to help in such discussions?

The second question is, are there any areas of concern that an SG or an AC continues to hold? And this follows on conversations that we've been having with the community, really, for the last year or 18 months in terms of outreach and engagement. So are there any continued concerns? What joint efforts can the CPH and other SGs/ACs engage in to investigate and address these issues?

And finally, looking at existing Contracted Party House efforts around botnets, malware at scale, etc., is there any additional clarity needed? Or can next steps be identified?

So those are just some preliminary questions, if anybody has thoughts about those or questions or responses. But again, if anybody has questions for this panel, please come on up to the mic. The floor is yours. Farzaneh, please go right ahead. Thank you.

SUE SCHULER: Please, we encourage everybody to put their hand up in the Zoom Room so that we can also include the people that are remote. I do have one question that came in for Samaneh earlier from Kristoff to [inaudible]. Is that 81% spam on slide four? Spam is defined in the DNS abuse definition.

SAMANEH TAJALIZADEHKHOOB: That spam has a delivery mechanism. So delivery for the other type of threats like malware and phishing and botnet command and control.

BRIAN CIMBOLIC: Okay. Thank you very much. Okay, Farzaneh, and then we'll come to Mark. Thank you.

FARZANEH BADII: Thank you, Keith. Farzaneh Badii speaking, NCSG. First of all, from Samaneh's presentation, we can agree that, basically, cyber

doomsday is not here and the situation is not as bad. I've been to too many DNS abuse meetings this week. That is my conclusion, of course.

The other thing is that when we discuss DNS abuse, we talk about tools, we talk about all kinds of initiatives to take domain name down. I think that we don't talk enough about governance processes that should be in place to use those tools—NetBeacon. I also think that as the measure of success, we focus on domain name takedown. I think it's one of the measures but we need to look at this more holistically.

Another point is the digital rights we need to look at, and that's our job at NCSG to tell you, of course. But if you can be aware of also, if you can in your studies and in your investigations, if you can consider structures that can protect digital rights while you're doing this great work of fighting with abuse, that would be great. I would like to see a discussion about that, the processes that are in place or that we can come up with.

As to Keith's question about engaging with other actors, I think that is a very good point. This is something that adds ICANN, unfortunately, because while ICANN is here and everybody comes here, they just ask the registries and registrars to do something about DNS abuse. But DNS has many actors and operators on it that they are also involved and we need to look at this more holistically and map these actors, and because sometimes registries and registrars cannot do anything about it. And yeah, that's it. Thank you.

KEITH DRAZEK: Thanks very much, Farzaneh, So I think Brian and Alan would like to respond. So, Brian, over to you.

BRIAN CIMBOLIC: Thanks, Keith, and thanks, Farzaneh. So I agree. We're obviously in an atmosphere where people want registries and registrars to become "more aggressive" on DNS abuse. But aggressiveness for its own purposes can be dangerous. So the other side of the equation is making sure that if you're going to be aggressive on DNS abuse, which I think is generally a good thing, of course, we're very out there on our stance on abuse being bad, then you need to be mindful of the impacts it has. So if you're lowering your threshold for determining when it's appropriate to suspend a domain name, then at the same time, you need to have robust processes in place that the registrant can reach out to you and say, "I think you made a mistake." I think that my domain name was compromised, whatever the issue is, so that the other side of that equation is observed so that you're not leaving a wake of collateral damage behind you. It's good to try and find and crack down on DNS abuse but you have to be thoughtful about the way that you go about it and build in protections, so that exactly your point, registrants aren't unfairly burdened by that decision.

ALAN WOODS: Thank you very much. Yes, again, thank you very much, Farzaneh, on that. What I will just add—and I suppose I segue in from what Brian was saying there—is another core element and something that we have tried to develop over time, and it has taken time, but it is figuring

out the evidence-based approach. So it's not only about ensuring that there's a process in place, but ensuring that what we're doing, and if we do take actions, that it is both transparent and it is certainly able to be demonstrated as to why the action was taken. I think that amount of clarity in the process, specifically how you do it, taking account of due process, and ensuring interoperability that the right party at the right time is taking the right action are all super important as well.

Then just mapping in and tying in that concept as Brian touched off as well is focusing from our point of view on malicious registrations and being able to ensure that we have a very sensitive approach to the compromised domain. Again, just harking back to the plenary, the last ICANN, specifically about compromised domains and ensuring that we are looking after victims, not just the end user victim, but also the victim who is the registrant in that compromised situation. So I completely agree with Brian and it is a patchwork of ensuring fairness in the process.

KEITH DRAZEK: Okay. Thanks very much, Brian and Alan. Just letting you know I'm having some connectivity issues with the Zoom Room. So I may need some prompting with who's next in the queue. So I know I've got Mark Datysgeld at the microphone. Sue, who's next?

SUE SCHULER: Next is Volker.

KEITH DRAZEK: Okay. Sorry, folks, we're following the order in the Zoom Room with the hands up. So, Volker, you're next. Go right ahead.

VOLKER GREIMANN: I like what I heard so far, and especially I like the initiative of netbeacon.org and abusetool.org, let's name them. But I wonder if we could not combine those efforts. I mean, one-stop shops are the kind of thing that abuse reporters are looking for. If they can have the services of abusetool.org and link to NetBeacon on abusetool.org, that would make the lives of the reporters that much easier if you can tell them, "Look, this is hosting, you might want to go there." This site has that information or you query that directly. So cooperation between different tools instead of competing tools or tools that complement each other but are not referenced, that will be very helpful, I think.

KEITH DRAZEK: Thanks very much, Volker. Reg, over to you.

REG LEVY: Thanks. Volker, that's an excellent idea. It had not occurred to me, and I don't know why. So yeah, absolutely. We'll put a link on abusetool.org to NetBeacon if it's a broader issue of abuse. And sure, the NSI will do something similar.

KEITH DRAZEK: Okay. Thank you. Who's next?

SUE SCHULER: We had a comment come in online. Also, glad to see the multilingual options for NetBeacon. It's interesting to see the traditional Chinese was chosen instead of simplified Chinese, which is more acceptable for reporters from China. Thank you.

KEITH DRAZEK: Thank you for the question. Graeme, I think I'll hand that one to you. Thank you.

GRAEME BUNTON: Thank you. Yes. Boy, I don't know actually personally a lot about how we implemented the translation on the website. I'm happy to find out more. It is important that we internationalize the service. I will say that the actual application right now is not translated. We still have some rough edges, I think, on the explanatory text to file off. Once we are happy with the content, we think it's explaining everything it needs to do, we'll get the application translated as well so that it's available and you can move from the website into the application seamlessly in the language of your preference. Thank you.

KEITH DRAZEK: Thank you, Graeme.

SUE SCHULER: Next in the queue will be Mark.

KEITH DRAZEK: Okay. Thanks, Mark. Thanks for your patience. Sorry about that.

MARK DATYSGELD: Thank you very much, everyone. Mark Datysgeld speaking, co-chair of the GNSO Council small group on DNS Abuse, but right now I speak in my personal capacity. So first of all, I would like to really commend the community on coming up with these tools. NetBeacon is very impressive. I didn't know about the tool that Reg showed us today but I've been testing it over here and it's actually pretty interesting. I really appreciate what it's doing.

I would like to just highlight one point about the data on DNS abuse, which I think has been addressed at some level in the presentation but I would like to stress it a bit because we have heard about how DNS abuse is going down, and I believe that is true. But at the same time, we might be looking into this from a certain perspective that perhaps this is a combination of spam moving to social media platforms and the introduction of different data protection laws, not only GDPR all coming into being at the same time and around this general period. So while I do believe that it's going down, and I do believe that the initiatives from the community are working. I'm slightly skeptical to say that we are seeing a massive drop. Perhaps we are seeing a discrete drop with caveats.

So as we move on with these new tools, as we find new ways to report, find new ways to aggregate the data, I would be a little careful and would like to see how we see the strands coming up and down so we can have a firm perception of what the threat landscape looks like in the longer term. So more of a broad comment, something that I would

like to have. If anybody has any reaction as well, I would be very glad to hear it.

KEITH DRAZEK: Thanks very much, Mark. So could you just restate the question just right at the end so I know who to hand it to?

MARK DATYSGELD: Perfect. Are we possibly seeing the reflection of a series of external factors affecting the data dramatically? And abuse hasn't dropped by half, but rather it's declining but not to the extent that we can see in those graphs that would be the ideal.

KEITH DRAZEK: That's great. Thanks so much, Mark. I appreciate it. Reg, if I can hand that over to you, and then to Alan.

REG LEVY: Thanks. Yeah, that's actually an interesting perspective and part of why the definition is so important. It's not necessarily the case that abuse worldwide is down. It is the case that DNS abuse is down. I know for a fact that my SMS abuse is going up and my spam phone call abuse is also through the roof, which is super fun in a foreign country. So yeah, you're absolutely correct. And it's not something that we're turning our eyes away from at all. But it is also definitely DNS abuse is down, and we are continuing our efforts to keep it at that level.

ALAN WOODS: I don't want to add too much to what Reg said, but what you did say did kind of resonate with something with me. And it was actually seeing Mason standing in the queue. His CircleID article recently where he said, "If abuse is going down, why would we be still talking about it?" I think the answer to that is, is because finally, I think we're in a position where so many things are occurring, quiet burns of efforts that are looking for sustained and proper action that is going to lead to change. I think that change is now becoming represented.

Can we do more? Yeah, I think that's something that we're all talking about and I think we are accepting. But where we're at at the moment is that we're now seeing the fruits of the hard labor that we've had over many, many years. And the fact that we are talking about it more is a very positive thing. I look forward to continuing on. So I agree with your point. I think it's getting better. We're not there yet but we're getting.

MARK DATYSGELD: Thank you very much, everyone.

KEITH DRAZEK: Thank you, Mark. Next?

SUE SCHULER: Next in the queue is Fabricio.

KEITH DRAZEK: Okay. Fabricio, go right ahead. Thank you.

[FABRICIO VAYRA]: Hi, everyone. I hope you can hear me from there.

KEITH DRAZEK: Speak up just a little bit, if you could. Thank you.

[FABRICIO VAYRA]: Awesome. Can you hear me now?

KEITH DRAZEK: Perfect. Thanks.

[FABRICIO VAYRA]: Awesome. So I just wanted to congratulate everyone up on stage. Awesome news, awesome initiatives, great presentation. I just wanted to ask, for all of you who are doing these great voluntary initiatives, how do you feel about the fact that sort of the rest of the ecosystem is able to operate without having to invest or do these efforts? And I guess in the case of bad actors, let's call it, haven registrar or registry, they sort of get to operate without any impunity. I mean, wouldn't you all prefer that there'll be a level playing field overall in the ecosystem?

I heard the prior speakers—a level playing field would actually help. Farzaneh talking about the fairness on both sides, sort of how we do or don't do things. Volker talking about sort of more unified, simple, less splintered approaches. And Alan, even you saying we're getting to

a point where we can see more sort of sustained or normalized ways of dealing with this. I mean, wouldn't the next step be to take these efforts and normalize them or run them through sort of unified contracts so that you guys are constantly having to carry the water for the ecosystem, and there aren't any questions about how things are splintered or dos or don'ts?

KEITH DRAZEK: Thanks very much, Fab. Anybody would like to respond to that?

BRIAN CIMBOLIC: Yeah. I can jump in. Thanks, Keith. So it's an interesting question, Fab. Yes. I mean, clearly, the parties on this in the abuse working groups, not just those on the panel here today, put a lot of time and effort and resources into responsible abuse practices. And yes, is there, admittedly, some frustration that there are those that don't hold themselves to the same standard? I think yes. If you're responsible registry and registrar, you put time, effort, and materials into these practices that we all think makes sense, we advocate for, and you see someone not doing that, does that make you frustrated and put you at its sort of competitive disadvantage too from a business perspective? I think the answer is yes. So I think it's kind of for us to take a look at how do we talk about the bad actors not in the room. We've had this conversation for years now. It's something that we're thinking about, and so it's a fair point. And yeah, thanks for bringing it up.

KEITH DRAZEK: Okay. Thanks, Brian.

SUE SCHULER: Mason Cole is next.

KEITH DRAZEK: All right, Mason, the birthday boy. Thank you.

MASON COLE: Thank you. Well, I'm not going to be embarrassed alone. Jothan Frakes's birthday is coming up soon, so happy early birthday, Jothan. I know he's in the room as well. All right. Thank you very much for recognizing me.

I wanted to follow up a bit on what Fab just said and I have a short statement. By the way, I serve as chair of the Business Constituency but this is in my personal capacity. So I and others are grateful to our friends in the Contracted Party House for their laudable voluntary efforts to combat abuse. Our oft stated concern, however, is that these efforts don't reach fully across the DNS to reach those who actively harbor the bad guys. Accordingly, I and others are on record advocating for a very limited set of contract updates that will equip ICANN Compliance with the tools it says it needs to properly enforce against abuse. We believe this is in line with advice from the SSAC and from the GAC dating back to the ICANN57 Hyderabad communiqué. We call on ICANN to initiate proceedings with its registry and registrar partners to proceed on this basis. Finally, based on experience and my own experience as part of a registrar and a registry, we don't make this recommendation lightly knowing that amending contracts can be disruptive. However, we believe this would be necessary and effective

tool for the Compliance Team says needs to help address this growing problem. All right. Thank you.

KEITH DRAZEK: Thanks, Mason. Go ahead.

ALAN WOODS: Thanks very much. Thank you very much for the insight on that one. I think Brian probably preempted what I would say here, and I think there is a sense of frustration in that. If I can refer back maybe to the Registry Stakeholder Group's submission to the GNSO's small team on abuse where we said, "Look, we are fully invested in the multistakeholder process and I think that what we need to do is be creative in how we're approaching this now." It's clear that there are those elements within the industry that are unhappy with the way that things currently are and there's probably a frustration on our side that we need to see how can we make things better. So the ability for us to pivot and the ability for us to be able to contemplate the multistakeholder in process, how we are as contracted parties, and how we can interplay them together is I think of vital importance to us.

There was a huge thread throughout this entire week and we're hearing this from the GAC, we're hearing it from the BC, from the IPC as well, and from yourself, and I think that we're all singing from the same hymn sheet to an extent. But we need to have a very serious thought about how can we do this effectively? How can we do this in a very focused manner? And how can we actually help ICANN as well to be the people who are helping us move this process along?

I think this is the beauty of being back face to face as well, this concept of being able to have these conversations. So much work, I think, has been done this week. I think we're all on the same page for once. I'm really happy and I'm excited to see where this takes us.

MASON COLE: Thank you very much.

KEITH DRAZEK: Thanks, Alan. Thanks, Mason. Sue?

SUE SCHULER: Thomas Rickert is next.

KEITH DRAZEK: Thomas Rickert. Thank you.

THOMAS RICKERT: Thanks very much, Keith. Hi, everyone. Thanks for the great presentations. I'm going to say a few words to the first bullet point about initiatives followed by a question. As some of you may know, I'm with eco Internet Industry Association. It has more than 1,100 members for more than 60 countries. 150 roughly out of these are in the domain space, but there are a lot of other types of internet infrastructure providers, hosting companies, CDNs, and others amongst eco's membership. Therefore, we formed the top DNS initiative in order to have a broader discussion about abuse.

For a man with a hammer, everything looks like a nail. And at the moment, it looks like we're perceiving contracted parties taking action as the silver bullet against all sorts of abuse. I think that's not appropriate, it's not proportionate for registries and registrars to take action upon all types of abuse. So I think that we need a holistic approach at tackling abuse. Becoming faster I think it's certainly an issue that the contracted parties need to look at. Because even if everyone is responsive with the recent change that we have, it can easily add up to a couple of days until you have a response. So I think these are things that can be worked on. But I would caution against this notion that if only the contracted parties did everything quicker, that we would solve all the world's problems.

What we've noticed in our discussions with hosting companies in particular is that we really have two parallel worlds. We have the ICANN bubble, and then we have the real-life discussion. So if you talk to the abuse departments inside hosting companies about DNS abuse, they don't even know that term. They don't talk about DNS abuse. And if you talk to them about real life scenarios, that rings a bell with them. So I think we need to get better at talking to them in the language that they understand and find ways to work with them better.

So my question to you is, it's my impression that sometimes the contracted parties are perceived by the outside world to be stubborn or not willing to cooperate because you're pushing back on some of the requests that we're seeing in the ICANN world, which have to do with ICANN's limited mandate and ICANN should not broaden this mandate, but how are you going to square the circle? Explaining how much you're doing with all the initiatives that we are today, and at the

same time, making sure that we don't have any mission creep at the ICANN level?

KEITH DRAZEK: Thank you very much, Thomas. Great questions. I think your point about ICANN's mission, ICANN's Bylaw restrictions, is a very important one. And we need to be very, very clear about what we can do within the ICANN space, but then also work to reach out to other parts of the ecosystem to ensure that as we deal with our own house as contracted parties within the ICANN space, we're engaging with others that have their own roles and responsibilities as well. Would anybody like to respond with this?

REG LEVY: Sure. I can speak to what I'm doing. And it's a good idea to reach out more to the combination—sorry, my brain just went—combination hookah and coffeemaker because I watched Aladdin way too many times as a child—the combination registrar and hosting companies who are in the Registrar Stakeholder Groups who make sure that we're using the right language. That's absolutely a great idea. So I'll be doing that in the DNS Abuse Subgroup.

Also at Tucows, we are doing our own DNS abuse initiatives trying to get data about resellers so that we can educate them about what kinds of things are causing abuse, whether it's DNS or not, and what they can be doing to avoid that in the first place so that it doesn't start. Somebody in the chat mentioned low value domain names. Yeah, absolutely. If you give away domains for free, guess what? You

get abused. And we ran into that with a couple of resellers. These are problems that we are addressing on the micro level. I say that as just one company. This isn't something that the Registrar Stakeholder Group is doing. But there are definitely initiatives that are not being presented here.

BRIAN CIMBOLIC: I'll just chime in on the registry side. I agree with you, Thomas. I think that there's a few things you can do. So one is akin to transparency reporting—you don't have to call it that, but putting out there—and for registries and registrars, I do think it's in our best interest to be very public about the things we're doing. Talking about the things we're doing not just on DNS abuse but taking a step back, I think that there's an erroneous assumption that people think when we say that, "Contents not within ICANN's remit, therefore, we're not going to touch content," that's not necessarily true. What we're saying, PIR—use us as an example. So we're obviously very aggressive when it comes to DNS abuse. But we also have partnerships with organizations on child sexual abuse material. We work with the U.S. Food and Drug Administration on opioids. There are some categories of limited instances of website content that we've made the determination that it's appropriate for us to take action in a reasonable way that builds in safeguards and due process.

We do that recognizing that it is not within our definition, DNS abuse, and it falls outside of ICANN's remit. So I would encourage people to recognize that just because contracted parties, registries and registrars, yes, we point to ICANN's Bylaws because it's clear in the

Bylaws, that content is outside of its remit, ICANN has stated that pretty unequivocally several times in the last few months. But that's not the end of the sentence for us. Our businesses, our operations don't end at when these ICANN meetings end. We go home, we mitigate DNS abuse, but we also have implemented varying practices to deal with certain limited instances of website content abuse in a responsible way and recognizing our place in the DNS.

ALAN WOODS: I just want to chime in one very small thing as well. Just a shout out to the SAP 115 paper as well, specifically on your other point, and that was with regards to the other players who have a part to play as well. And that's absolutely agreed. Interoperability is one of those things that we need to be exceptionally mindful of as we proceed in this. I think I said it earlier. Again, it's the right option by the right party at the right time. I think we need to keep pulling on those threads of including the other elements of the broader Internet. It's not just registries and registrars, there are many layers involved.

KEITH DRAZEK: Thank you for the question, Thomas, and thanks for the responses. Just a time check. We have about nine minutes left in the session. I do not see anybody in the queue at the moment but I know that we've got a couple of questions that were submitted in chat. So if I could turn to Sue.

SUE SCHULER: We do. A question came in for Graeme from Steve delBianco. "It seems like NetBeacon can only accept reports if the domain provides RDAP response. Does that enable bad actors to avoid investigation?"

GRAEME BUNTON: Thanks, Steve. I think I'd have to see the example because that shouldn't be the case. We are limited at the moment to gTLDs. So if you're trying SEC, that could be an issue. But please send me the domain name and we'll look at it. Thank you.

SUE SCHULER: Okay. Then a second question from Steve, "The data presented said that domains hosting abuse has declined. But the instances of abuse from those domains may well be increasing. Are we measuring abuse correctly?"

KEITH DRAZEK: Thanks for the question, Steve. Let's see if anybody has a hand up.

REG LEVY: I can take a stab at suggesting that that's a question for Mark. People, like security researchers who gather that data, the retail block lists that are collecting this information would be the ones to send that out to. If there is a phishing website, you're right. I don't know if one person clicked on it, 100 people, 100 million people. It's just one website. So maybe we aren't sure. But this is how it has been counted for some time so it's going to be very difficult to change all of our metrics suddenly and get any reasonable information out of that. At

least looking backward, but perhaps moving forward. If you like to come up after the meeting, I can introduce you to a number of security researchers and you're welcome to put that question to them.

KEITH DRAZEK: Thanks, Reg. I now have Paul in queue, and then Terence. Paul?

PAUL MCGRADY: This is more of a statement than a question and it's in personal capacity, of course. But I just wanted to say thank you. For years, we struggled with the in-scope and out-of-scope thing and now we're seeing a lot of movement and people within the community doing things that perhaps their ICANN contracts don't require but it's looking out for the little guy at the end of the day. I think that one thing we can do without violating the scope issue is that we can cheer for each other when we see people trying new things and trying to solve things. So I'm here to cheer for you. Thank you.

KEITH DRAZEK: Thanks very much, Paul. Much appreciated. Good work has been done. There's more work to do, and we're committed to that. Terrence, over to you. Thanks.

TERENCE EDEN: Thank you. Terence Eden from [.gov.uk]. We're really excited to see this and we look forward to both receiving reports and sending reports. It's great that this has been promoted to registrars and registries. I'd like to ask what's been done to promote it to the general

public. And I'd like to understand how this fits in with the other reporting tools, things like Netcraft and Google Safe Browsing. Is this designed to replace it, to supplement it, to work with those tools? Thank you.

GRAEME BUNTON: I'm going to assume that was for me, right? NetBeacon?

TERENCE EDEN: Yes, or anyone else who wants to answer.

GRAME BUNTON: Okay. We're learning as we've launched a little bit about exactly how the tool is working and how people are using it. So I think we've got a few more features and some bugs to fix and some rough edges to polish off before we really go about trying to engage with a very broad public and drive traffic to it. That's going to be straight up marketing, it could be like purchasing AdWords. In an interesting conversation today with some SSAC members, they were talking about working with e-mail providers and browsers to automatically route abuse reports to it. So we'll investigate all of that. We want to see how much of that we can capture as possible.

The tool not being an abuse management system, so it's not scanning all of the domain names that a registry or registrar has, and so we're not consuming full feeds to do that comparison. What we're doing is taking a domain name and checking it against a feed. So we will integrate as many of those sources of information as registries and

registrars find valuable, but it wouldn't replace them or even it wouldn't replace an anti-abuse solution that a registry or registrar should probably have in place. What it really does is help clean up that messy manual reporting that consumes a lot of time. Hope that helps.

TERENCE EDEN: That's great. Thank you.

KEITH DRAZEK: Thanks, Graeme. Terence, I think there's a couple of more responses to your question. Reg, I'll turn to you first and then Alan next. And then we'll come to Griffin for probably our last question. Thank you.

REG LEVY: Thanks. The abusetool.org is intended to be something that doesn't actually feed into NetBeacon or a registrar's review systems. There are no plans to do that. However, we encourage our membership to add it to their abuse pages so that when someone goes to a registrar to report something, they can click and say, "Actually, I should be recording this to a hosting company perhaps." And that is part of the outreach that we're doing to disseminate it because again, people get to the registrars and they get to the abuse page and then we can say, "Actually, maybe even embed it in our sites if we can do that."

ALAN WOODS: Just going back to NetBeacon, if they were to send a complaint through to the registry of the registrars, what happens after that? From my point of view, and I mentioned this earlier, is the concept of

the highly evidence case. So from Donuts' point of view who are my employer, we partner with CleanDNS to provide that. So we will take reports from anyone.

What's important for us, however, is the evidence that we can apportion to that. So you've mentioned Netcraft and places like that, they are indicators that we add to any report. We enrich those reports and we ensure that if ever we are to escalate or to take action, that that is fully evidenced, so that we don't escalate something just because we got a report and it's just listed somewhere. We escalate because we have the evidence that supports the, I will say, allegation being made. So that's a very important thing for us, is ensuring that it's evidence based but we will take reports from wherever.

KEITH DRAZEK: Great. Thank you very much. Griffin, over to you for the last question or statement, and then I'll turn it back to Brian or Reg for any last comments.

GRIFFIN BARNETT: Thanks, Keith. Thanks, everybody. Griffin Barnett for the record. I'm a member of the IPC but speaking personally. Thanks very much for this panel. It has been incredibly informative and helpful, I think.

The question I have kind of pivot to a related topic when we talk about abuse, and I know it's everybody's favorite other topic right now is WHOIS issues. But they are interrelated. Because often, there's a parallel process for reporting abuse and also trying to find out who's behind the abuse of domain. I guess my question is can you speak a

little bit to the interrelation between reporting something for takedown, for example, but also concurrently trying to find out additional information about the registrant or who's behind that domain, and how we might mesh these two pieces together in terms of takedown related requests, plus the other piece of trying to get to the WHOIS information so that we can conduct additional investigation and things like that? Thank you.

KEITH DRAZEK: Thanks, Griffin.

ALAN WOODS: When we get to that point—I'm just going to mention our provider. When the GDPR came in, the conversation we had directly with the CleanDNS was saying, "Look, the entire status of the way things were done has changed because of the legislative enactments in the world." And what we asked them to do was, "You know what, let's try and take that reliance away from WHOIS." Because let's be perfectly honest, for most of the time, we don't actually use WHOIS for our benefits. We've asked many times, "Well, what is the benefit of it?" I mean, sure, there are. But from our point of view, we tried to move away and trying to figure out, "Let's take the option based on the evidence." And the evidence I'm try to move away from this over reliance on something which is now a heavily legislated concept.

I understand the frustration and I hear what we're seeing from the IPC. But the fact of the matter is that the old methods of dealing with these things, we need to move and probably innovate a bit more in trying to

get away from that reliance on that. That's pretty much what Donuts does. We look at the other indicators. The indicators that are equally there. That is not necessarily the name of the registrants. But there are other indicators on that domain that we can see that are, as far as we're concerned, equally as important. That's the way we've approached it. I think it's time that we need to innovate, not look backwards.

KEITH DRAZEK: Thanks, Alan. We're just about out of time, folks. Thanks for that. Brian and Reg, if I could hand it back to you for any concluding remarks, and then we'll go ahead and wrap up, and then move to our next session. Thanks.

REG LEVY: Thanks, Keith. And thank you very much for moderating that. That was incredibly constructive. At least for me, and I know for most of the people on this stage, a very constructive conversation. So thank you all for your input and for being here in this voluminous room in which I hear my own echo. Have a great cocktail party outside because I think that's the time it is.

BRIAN CIMBOLIC: Great. Thanks, everybody. We appreciate your attendance and contributions. So have a great rest of your afternoon and evening.

SUE SCHULER: Thank you, we can end the recording now.

[END OF TRANSCRIPTION]