ICANN71 | Virtual Policy Forum – GNSO - CPH DNS Abuse Work Group Community Update
Wednesday, June 16, 2021 – 10:30 to 12:00 CEST

ANDREA GLANDON: Hello, and welcome to the CPH DNS Abuse Work Group Community Update. Please note that this session is being recorded and follows the ICANN expected standards of behavior. During this session, questions or comments will be read aloud as submitted within the Q and A pod. They will be read aloud during the time set by the chair or moderator of this session. If you would like to ask your question or make your comment verbally, please raise your hand. When called upon, you will be given permission to unmute your microphone. Kindly unmute your microphone at this time to speak.

All participants in this session may make comments in the chat. Please use the dropdown menu in the chat pod and select respond to all panelists and attendees. This will allow everyone to view your comment. Please note that private chats are only possible among panelists in the Zoom webinar format. Any message sent by a panelist or a standard attendee to another standard attendee will also be seen by the session hosts, co-hosts and other panelists.

This session includes automated real-time transcription. Please note this transcript is not official or authoritative. To view the real-time transcription, click on the closed-caption button in the Zoom toolbar. With this, I will hand the floor over to James Galvin. Please begin.

JAMES GALVIN: Thank you. And thank you to everyone for joining us this morning, afternoon or evening as it is, wherever you are. Welcome to our second CPH DNS Abuse Community Outreach Session. I'm joined today with my co-chairs. On the registry side, we have Brian Cimbolic and on the registrar side, we have Reg Levy and Luc Seufer. And thanks again to everyone.

Just to note here for how this will work, we are all working here today as co-chairs of this session. So, along the way, if any one of us raises our hand and wants to speak, we'll be allowing each other to jump the queue and speak out if we have something to add or comment on with respect to whatever's going on in the discussion.

So, with that, let's jump to the next slide here. We had such a successful session at ICANN70 last time. We've decided to do it again this time. Along the way, we've had quite a lot of success in activities that we've done and we're going to be speaking about all of that today and telling you about it, giving you an update on the work that's been done, work that's in progress.

And as we pointed out last time, we've been doing explicit outreach, the Contracted Parties as a joint effort to all of the SOs and ACs. And we've had first meetings with most of them at this point and we're just beginning to schedule second meetings. And, of course, this is our second meeting with the community at large and opportunity for folks to bring to us questions and respond to the questions that we have for you.

So, let's move to the next slide and we'll take a quick look at what we have gotten, some key takeaways from the outreach sessions that we've had so far. We have met with the NCSG once. That was really just a kickoff session with them. We just kind of had an interaction and an opportunity to chat with each other so there's no real key takeaway there. They really were just trying to set up an opportunity for us to understand each other and we expect to get more out of our second meeting with them.

We met with the ALAC and we discussed a lot about some potential education materials. As I'm sure most of you know, the ALAC has quite a success rate in preparing general materials that are useful to folks across the Internet, as well as in the ICANN arena. And we expect to kick off some opportunity to work with them quite directly in producing some additional materials, general education materials for the community at large.

With the IPC, our key takeaways there were a desire for an IDN homoglyph domain attack. We'll be hearing some more about that later. Incentive programs too. Registrars already had incentive programs in progress so it was good to have that opportunity and an affirmation that was interesting to them and we'll know more about that later. And we have a framework on trusted notifiers which was equally interesting to the IPC and the BC when we talked to them and we'll have an opportunity to hear more about that in our session later from work products.

Also, on behalf of the BC, a key takeaway was the desire for some expanded guidance on abuse reporting. And folks here will also recall that, there's been some energy in the ICANN community in general for responding to that issue.

In our community session last time—just to be clear, also similar to our meeting with the ALAC—was the desire for creating more resources, a better collection and organization, categorization of the work that we're doing. And so, we have actually just begun a process. Both the registries and the registrars have our own website for our resources and we're going to be expanding that.

And as we begin to build out our work products, which you're going to hear some more about here in a moment, we're going to put those materials there and also materials that we develop with the ALAC. We're going to provide a nice centralized location where other registries and registrars will each have a good source of opportunity for some guidance on, as from our work products that we're producing and also the community at large. Next slide, please.

And then the other thing that we've done is some upcoming plans. As we've already reported. We've had our first meetings that came after ICANN71. We're planning a meeting with ccNSO, ISPCP, and SSAC. We're just beginning to get those meetings scheduled. They each had their own reasons for delaying our opportunities to get together but we're going to get that taken care of. We're also reaching out for having our second meetings with BC and IPC so we're going to continue to progress these meetings, as we have things to talk about and an agenda

and can progress the work products or key takeaways as described in the last session.

And just to continue to point out, that we have ongoing meetings with PSWG and OCTO. We're going to be hearing about some PSWG work products here next. And with OCTO, we have had extended meetings with them in the past with respect to DAAR and we do expect to continue those discussions, as you'll see here on the next slide, as we move to talking about our Registries Stakeholder Group work products that we've been working on.

So, with that, one last logistical comment. If people have questions or comments, there is a Q and A pod and a chat room. Please feel free to type into the chat room and the Q and A pod as we go along, we'll be gathering those up. And at the end of all of our presentations here, our quick update from the various work products, we will go back and start with those questions and go through them and also have an open forum for folks to raise their hand if you feel that you want to speak and offer up your question or comment. So, with that, let me offer to the next slide, please and turn this over to Brian Cimbolic, my registry co-chair.

BRIAN CIMBOLIC: Thanks very much, Jim. Hi, everyone. As Jim mentioned, I am Brian Cimbolic with Public Interest Registry. I'm also the Co-Chair of the Registries Stakeholder Group DNS Abuse Working Group. I'm here to just provide an update on some of the work product that is being co-led by the Registries Stakeholder Abuse Working Group. And I say co-led because, as you can tell from these various outputs, the focus on the

work of the Registry Abuse Group has really been informed by our conversations in the outreach.

So first, just an update on our work on DAAR, the real predecessor of our group was the DAAR Working Group that worked collaboratively with OCTO to provide recommendations to improve that system that OCTO actually implemented. And we continue to look at DAAR reports and we continue to have that as a constant work track.

Flowing from some of the recommendations around general educational materials in the vein of our conversations with the ALAC, the very first document that we put out as an output from the Registry Abuse Group is the registry operator available actions. Our friend Gabriel Andrews from the FBI is going to speak to our collaboration with the Public Safety Working Group on the framework for DGAs, associated with malware and botnets.

Keith Drazek will speak to our work on the trusted notifiers, which really flows from our conversations with both the BC and the IPC. I'll touch on this. We have a working group dedicated to looking at outstanding CCT recommendations. And finally, Dennis Tanaka and Brian King will lead us through a discussion on an upcoming work track that's really a joint effort between the registries, registrars and the IPC and that is issues associated with IDN homoglyph attacks. Next slide please.

So, as I mentioned, the first real document that we put out as a Registries Stakeholder Abuse Group is the educational material in the vein of educational materials and this is the registry operator available actions. And what this does is, it's meant to give a high-level summary

of what it is that a registry operator can do when it's identified DNS abuse. Specifically, what should a registry operator do when it's faced with a malicious registration.

And this document very intentionally highlights the difference between maliciously-registered domains and compromised domains because the mitigation associated with a maliciously-registered domain at the registry level is necessarily going to be different than a mitigation for a compromised domain, in which the proper remedy really for a compromised domain isn't necessarily suspending, particularly at the registry level, but rather working down the stream, trying to get the domain, or control of the domain, or control of the web hosting back in the hand of the legitimate registrant.

Finally, this document tees up the distinction for maliciously already-registered domains and domains that will be maliciously registered, in particular domains that are part of a domain generating algorithm, malware, botnets associated with the DGA.

With that, we can go to the next slide and our friend Gabriel Andrews from the Public Safety Working Group will talk to the framework on DGAs that the Registry Abuse Group and the Public Safety Working Group recently published together that—I'll put a link in the chat—is now available at the Registries Stakeholder Group site. With that, Gabriel, take it away.

GABRIEL ANDREWS: Thanks, Brian. So, quick background on this point. It's going to be somewhat U.S. centric. My day job is law enforcement agency in the United States but this is identified as one of those areas that we, we being the Public Safety Working Group and the Registries Stakeholder Group felt was low-hanging fruit to address.

Now, let's start this off, just quick definitions of terms here so that we're all on the same page. When we talk about domain generating algorithms, what we're really talking about is the use of botnets by criminal actors. Now, botnets are networks of compromised devices that are typically controlled by criminals in the furtherance of some scheme or another.

And one of the ways that these botnets can be controlled is via the use of these domain generation algorithms. And all that means is it's a piece of code that you can take in as an input, some future specific date and time. It could be tomorrow. It could be a year from now. And it'll output a specific domain name that would be specific for that date and time. And that would enable all of those infected devices out there in the world to know that, "Hey, if we need the instructions and we reach out Christmas of 2023, we need to check this domain at that date and time."

And if the bad guy in the future registers that domain at that time, he can issue commands to his botnet which means that this is somewhat problematic for law enforcement to address because in order to address the criminals use of this botnet, we need to now somehow address all of the potentially hundreds of thousands of domains that could be output by this algorithm this year, next year, the year after

that. And so, necessarily, this is something that is going to be sort of low frequency and that we're not taking down these huge types of criminal botnets—the types that you might've heard—Conficker, Avalanche, these very large and very well-put-together organized criminal schemes.

But when we do, do a takeout of this nature, it's very high impact. It involves a lot of effort, both on the part of law enforcement, on our legal system as we go to the courts and chief authorities in order to seize domain names, and on the part of the registries that we work with as they work with us to take the action that's going to be most effective in this. It's work all around.

Complicating that, is that in the past, we've had to often go before a court on, say, an annual basis and say, "Hey, here's the list of domains associated with this year of 2020," and then do it again for 2021, and then do it again for 2022. And similarly, I'm led to believe that registries have sometimes had to seek repeat approvals from ICANN for authorities to take action or for fee waivers associated with their action that's taken in response and in good faith to law enforcement requests.

So, what we were seeking here, and what I think that we've achieved, is setting a framework of best practices that will identify the best possible path to achieving that kind of action that we seek to achieve here without requiring us to continually go back to the well to keep seeking those annual authorities, whether it be from the courts or from ICANN or what have you. And this is what Brian has termed an evergreen solution, where hopefully, it will tell law enforcement the type of

information that would be most useful to do one great referral that will enable continued action forever without the need to spend all these administrative resources addressing this very important issue.

With gratitude, Brian and others took this to ICANN and received some very positive feedback in terms of … I'm going to ask Brian to correct my understanding here but I believe they were suggesting that registries could even take more action sooner without approvals than we had initially listed in our document. And so, it was very forward-thinking and positive support from ICANN in this regard. But we are very hopeful now that if we can have folks refer to this framework as shared best effort at best common practices, that this will reduce our joint efforts in the future. And Brian, I'm going to ask you or Jim to fill in any gaps and blanks in what I may have just covered here and add your own perspective to this effort.

BRIAN CIMBOLIC: Thanks very much, Gabe. No. I think you hit the nail on the head. And as you alluded to, yeah, this is a real area of … One, it shows the continued track record of cooperation between the registries, registrars and the PSWG, particularly dating back to the security framework. And we're continuing to look at those areas of low-hanging fruit. What are the low resistance, high impact things that we can work on together? And we're going to continue to look at those.

And as you mentioned, ICANN, especially, because our framework touches on going and communicating with ICANN—the registry getting permissions for waivers of certain parts of our contract, for example, to

create a domain name. There's a contractual prohibition for a registry to just do that on its own without working with a registrar. And when you're dealing with a botnet that requires specific timing across a number of registries, typically, the registry has to do that on its own.

So, we looped in ICANN and ICANN was very cooperative and, as Gabe mentioned, actually wanted us to specifically include the notion that registries are free to address these botnets first and use the ERSR system, the Expedited Registry Security Request and get the waiver retroactively. So, real kudos to ICANN and working with both the PSWG and registries cooperatively on this. So, thanks very much, Gabe, and we appreciate you especially getting up to join our panel at oh dark thirty in California. So, many thanks, Gabe. Next slide please.

And with this, Keith Drazek, if we could hand it over to you to touch on the framework on trusted notifiers that's in progress.

KEITH DRAZEK: Okay. Thanks very much, Brian and hello everybody. So, yeah. Just a quick update on the framework for trusted notifiers. The Registries Stakeholder Group DNS Abuse Working Group and the Registrars Stakeholder Group DNS Abuse Working Groups have a joint effort underway to develop an outline and a framework for discussion on the topic or subject of trusted notifiers.

This is in part in response to outreach and community concern about the need for clarity around the use of trusted notifiers. And the goal of the Contracted Parties in this area is to help frame the discussion

around trusted notifier relationships to help establish expectations of behavior, expectations of action, the expectations of a trusted notifier and then to better understand what the capabilities of a contracted party are in reacting or responding to such trusted notifications.

So, this is really in the early stages of our internal discussions within the Contracted Parties but I think the key point here is that we really do look forward to taking this discussion to other parts of the ICANN community—to the broader ICANN community—to better understand what the expectations might be around such trusted notifier relationships.

I think it's important for us to note that in our thinking, we're not necessarily looking for this to be any sort of an ICANN program at this point and perhaps not at all. We recognize that there are topics related to DNS abuse, the technical infrastructure abuse that we're focused on today. There could at some point be opportunities for engagement on things related to content beyond infrastructure abuse but that's really outside the bylaws and the mandate of ICANN. But I think that this framework and the discussion on trusted notifiers will help us as Contracted Parties engage with other parts of the ICANN community to really better understand what the expectations might be about those relationships.

And ultimately, I think it's important just to underscore that any type of a trusted notifier relationship is still going to be a bilateral relationship between the contracted party in question and the trusted notifier in question—that it ultimately will be up to those entities to establish the

framework for their bilateral engagement. But we're really hoping that this framework will help establish, essentially, the common expectations or common understandings, maybe a minimum threshold of expected engagement and expected standards. So, we really do look forward to continuing this conversation both internally and also with other parts of the ICANN community.

Brian, maybe I can hand it back to you if you'd like to add anything to that or to, of course, correct me in any way necessary. Thanks.

BRIAN CIMBOLIC: No correction necessary at all. And many thanks, Keith, for taking the reins on this one. We certainly appreciate it. Next slide please. So, this is a working group. The registries have recently kicked off a working group to take a look at the CCT recommendations. This is admittedly a newly formed group. I think we've met two or three times over just the last month and a half or so. And it's very ably chaired by Jeff Neuman who is unable to join us because of his obligations with the GAC. But this group speaks to specifically take a look at the recommendations as they relate to DNS abuse—in particular, what has already been implemented and have there been any sort of community work that has potentially filled a gap in a specific recommendation.

So, this work is early on but we're excited about it. We understand that these recommendations continue to be a topic of conversation recently. I know that the GAC had specifically touched on these. So, it's something we're paying attention to and hope to have a more developed update by the time ICANN72 rolls around. Next slide, please.

And with this, I will hand it over to Dennis Tanaka and Brian King to talk about the IDN Homoglyph Attacks Working Group.

DENNIS TANAKA: Thank you, Brian. So, yeah. This is a joint effort that we are going to take, along with the IPC and a small group of volunteers as well. But let me start off by saying that internationalized domain names and the underlying component, Unicode standard, really enhance the linguistic diversity on the Internet, as it enables millions of users and many more to use their own language and scripts to express themselves on the Internet.

But as any product feature that is really is created for good use, I mean there's always bad actors that want to use it in different ways. And therefore, we're talking about IDN homoglyph attacks, which is also known as script spoofing, in which they use the characteristic of Unicode letters that look alike with others in order to deceive users by creating labels that might be otherwise a different domain name.

So, as Brian alluded earlier, this is a concern of shared interest with the IPC. So, Brian King and I, will be leading this working group to look at the issue, quantify the problem, and also offer a sort of educational framework for all the registries and interested parties to knowing what the scope of the problem is, what resources are available within ICANN and outside ICANN in order to be informed about how to mitigate these types of issues. Brian King, do you want to add anything or correct me?

BRIAN KING: Sure. No, corrections, Dennis. Thanks. I'd like to echo a lot of what Dennis said including … The first point, I think, is that we start from a place of being supportive of IDNs and all the good that they provide to the DNS and the opportunities for people who don't speak English or use alphabets that use the Latin character set and we remain supportive of that as a starting place for this research.

And with that being said, I think there is research to be done, right? As Dennis alluded to, we need to identify the scope of the problem, the potential problems here and the potential policy solutions that could help prevent these types of attacks. I thought too late of perhaps a dramatic slide show here where we took out the Punycode there and just ask the audience to pick which of those domain names was the real icann.org, with the surprise twist being that neither of them was and how you would actually represent icann.org in Latin—in the standard 26 characters, A through Z, Latin alphabet.

So, I think this does really point to the believability of some of these and I think we can hope to take advantage of a lot of the good work that's been done with Unicode and with other groups on which characters have been flagged as confusables and see if there's a policy solution that might prevent some of these attacks.

So, a lot of work has already been done here through the IDN guidelines developed by ICANN. I note that there's a new version that's not yet in effect. And so, there's an opportunity really for us to stand on the shoulders of those giants and perhaps come up with some interesting

policy applications here. That's all for me. I'll turn it over to the other Brian.

BRIAN CIMBOLIC: Thank you, other Brian. Next slide please. And actually with that, I will hand it over to our friends in the Registrars Stakeholder Group Abuse Group. So, I think Reg, if it's you, take it away.

REG LEVY: Yeah. Thanks, Brian. And welcome, everybody. We appreciate you joining us for this session. The slide that's on the screen right now, you will get in the final outputs. Briefly we're going to go over what we have done and what is in various stages of process. Next slide, please.

So, we have a number of already published papers, which I'm going to drop into the chat, including our guide to abuse reporting which includes everything that a registrar needs in order to take action on an abuse complaint. So, very often we get malformed complaints and so we aren't actually able to take appropriate action or confirm that the abuse has happened.

We additionally have published a paper with regard to how the registrars reacted to the influx of domain names including the phrase coronavirus, and COVID-19, during the first part—probably the second quarter actually—of 2020. And what it found, in fact, was that a lot of the domains that were registered using those keywords were beneficial or simply parked. So, it was an interesting insight into what often people think might be abusive but turned out to not be.

Finally, we have a minimum required information for WHOIS data requests, series of questions. And this has been developed in the Registrars Stakeholder Group to help people who are looking to have previously public WHOIS information disclosed to them. It's a series of about seven questions that include who the requesting is party is, what the legal basis for their request is, and assurances that they will dispose of the information after it has been used in the manner that is described in the questions.

Again, I put those into the chat box so if anybody wants to read those or access them, they may do so. Next slide, please. Thank you. And now I'm going to turn it over to Ashley.

ASHLEY HEINEMAN: Hello, everyone. Ashley Heineman here with GoDaddy and also the Registrars Stakeholder Group Chair. I'm going to talk very briefly here about a work item that is underway right now and it's looking specifically at incentive programs for combating DNS abuse. This is something we started working on some time ago when my predecessor, Graeme Bunton, was filling my shoes as well as that as the DNS abuse subgroup chair for the Registrars Stakeholder Group. And it's basically recognizing, first of all, that this is an area of interest in the community.

And so, we figured since it's impacts us directly, that we would kind of get a jump on things and draft essentially a discussion paper that frames the key issues and attributes associated with these types of programs. But in this vein of not wanting to work in silos and at the early outset to get input and perspective from the rest of the community, we

wanted to get some input from folks to inform how we proceed in developing this discussion paper.

So, rather than provide you with a draft as it is now—because it needs some work. It's a bit dated. We're going to get it up to speed here. We wanted to go ahead and ask you all now these questions. And we have a link here that will assist you in providing any input. And as you'll see, these are some very broad questions because we are at the early stages including like, are these types of programs desirable? I'm guessing the answer is probably going to be yes for many of you. What protections should be in place for registrants? Because that is something of concern, particularly as these are our customers. And what aspects should be considered for an effective incentives program?

So, any input we receive from you all, we'll be sure to take under consideration as we further flush out this paper but again, it's intended to be for discussion purposes. And our ultimate goal is to have this be reflective of the registrars' perspective of what makes a good incentivization program so we can get this to ICANN, should we get down a path where they consider doing something like this so that they know what our views are moving forward. So, I will stop there and I believe turn it back to Reg.

REG LEVY: Thanks so much, Ashley. Next slide, please. And for registrant protections, I'm going to turn it over to Owen Smigelski at Namecheap.

OWEN SMIGELSKI: Thanks, Reg. I'm with the registrar Namecheap and I'm also Vice Chair for policy for the Registrars Stakeholder Group. So, with this whitepaper that we've been working on here is, various protections that can be there to protect registrants with regards to abuse.

And just want to highlight that this is not intended to facilitate, foster, or protect abuse. I would say it's to give a due process and realize at the other end of an abuse complaint, there is somebody who's registered a domain name and there may be a possibility that it may not be that person's fault, or they may not be responsible, or what action they can take to protect themselves if their site is shut down. Generally, from a registrar, registries perspective, the only thing that can be done is to completely shut down and suspend a domain name, as opposed to taking a page offline that may have been hacked or something along those lines.

So, this paper highlights some of the protections that are there to ensure that registrants need to have the due process. And the first one in there is that all DNS abuse complaints should be based upon material, actionable reports with verifiable evidence. Quite often, from a Contracted Parties position, if we're seeing this abuse complaint, we may not be able to see it. There are certain types of abuses that target certain geographic regions via IP address. So, if somebody is noticing the abuse in, say, Japan, it may not be visible to somebody in the United States. So, having that documentation can ensure that if we take action to break a contract with our customers, that there is a good and justifiable reason for doing so.

The next type of appeals process are ones that are internal through the contracted party. This can be an escalation through a customer support system or some other thing like that. But just giving the opportunity for the customer to know what happened to them and why and for them to either rebut or provide additional evidence about why this should not be allowed to stand.

And just as a caveat, this does not mean that every single abuse complaint can go through these types of actions. Quite often, say, a law enforcement or other type of sensitive abuse complaint is involved. These are things that are often just not communicated to a customer at request of the reporter. And also these are not mandatory things. These are things that are optional, that a registrar or registry may do and follow, but it's not something that they have to do.

The next one is some type of internal ombuds, which is independent third party who can review and kind of give a new, fresh look at something, as opposed to, quite often, the abuse teams, like the customer support flow, are also the ones who are involved in taking down the abuse in the first place. So, having that independent third party can ensure a little bit more check on there and make sure that everything was followed in there.

And a final item in there is kind of loosely called courts of competent jurisdiction. Those are outside opportunities to appeal, either through public ombuds in some countries, consumer agencies, law enforcement, perhaps through ICANN. And yes, also through law enforcement, if there was some type of inappropriate action taken by a

registrar against taking away domain name or other type of valuable content.

This is this last note here. This draft paper has been presented to ALAC, NCUC and the PSWG and we've solicited feedback. We're waiting to see if we get some of this before finalizing and publishing this paper. Thank you.

REG LEVY: Thanks, Owen. Next slide, please. And now I will turn it over to Theo Geurts.

THEO GEURTS: Thank you, Reg. I'm with [inaudible] the incident response team at Realtime Register. That's a registrar. And the Registrars Stakeholder Group has been working on a whitepaper on the business email compromise for a while now. We're not exactly finished. When I was going through the material, I noticed that we could add a few more things on the technical side as well.

But basically, when we are talking about BEC fraud, we are talking about hacking humans, hacking people using techniques like impersonation, deception, and a little bit of social engineering as well. It is not as frequent as phishing attacks but the impact of BEC is quite high. The efforts BEC attack yields a cybercriminal around $85,000. So, that's quite high for the victim and society and it is definitely something that is in the realm of DNS abuse, as the delivery vehicle is mostly done by email, not always. Sometimes through postal mail or voice. But

when we are talking about whitepaper, we focus on the email aspect and it's quite hard to detect it but there are some stuff that can be done.

And usually, when we are talking about the BEC fraud, we are usually focusing on what I call the shotgun approach, which is where a large number of emails are sent to employees of a company. We are not talking as much in the whitepaper about the highly-sophisticated BEC attacks or the BEC attacks that happens through cloud computing, etc., etc., that's all out of scope. So, we focus on the business email fraud attacks that we usually see.

And what happens is usually an employee receives an email from his or her CEO with the order to send money to a law firm because there is a fantastic opportunity for the company. The employee is under secrecy, is not allowed to tell anybody. And usually that pushes a lot of buttons with a lot of people, depending, of course, on the company culture, on the status of the CEO. In some countries, it is very usual that such order from a CEO are carried out as a good soldier.

So, depending on the environment, these attacks can be very successful. What can registrars do? Not a whole lot from the technical side because BEC or email is within the DNS but it's not technically part of the—or in the same realm as the registrars. But what is very successful is when you apply to your existing procedures, something like an incident response-based approach that you map out, document stuff, usually when you do that, you can come to the conclusion. Or in our case, we did find a phishing network for bank fraud and we did find

a network of criminals that were actively abusing our platform to conduct BEC fraud.

There's also, we talk a little bit in the whitepaper, a little bit about tooling. We don't go too deep into that because it varies a lot on the registrar, the business model, the knowledge on how to use these tools. Personally, I use a variety of tools like [inaudible].com or Maltego or SpiderFoot. But like I said, it highly varies among registrars.

And lastly, we talk about what can you do to prevent BEC fraud? And it basically boils down … When we talk about BEC fraud, it's pretty much low-tech for the most part but we can see if you start implementing procedures, you start educating your employees as a company or organization, you start training people and you make sure that your people are being tested, that is basically your first line of defense and prevents most of the issues when we are talking about the business email compromise. From then on, you can, of course, implement technical supportive features but basically what I just mentioned is your first line of defense. And I expect the paper to be released this year, hopefully soon-ish but it's in the works, folks. Thanks.

REG LEVY: Thanks, Theo. Next slide, please. So, the in-topics of abuse … Actually, I think this is me but somebody else was supposed to do it, I apologize if I'm stealing their thunder. Topics that are currently in progress for the registrars … This is Luc. Sorry. Luc. I will turn it over to Luc.

LUC SEUFER: Hi, everyone. Okay. So, yes, the DNS abuse triage tool is still a project under discussion but the main specifications are already defined and the cost is known. So, the tool is based on the definition of abuse from the frameworks—so, malware, botnet phishing, pharming—and the plan is to make it available on the ASG website. It will be for cases where registrars can take action but are not always best suited.

So, you will have to close your eyes and imagine a regular search box because I have nothing to show you right now. It's still a project. But once you enter the domain name involved in abuse, you will have free set of data that can be retrieved, which are the ones on your screen. And rather than trying to explain technical things that I barely understand, I will take regular or semi real-life example.

So, for the email service provider details, those details are useful for spamming cases. Let's take the case of a plumbing company that registered a domain name. They create a website and they choose Microsoft 365 for their email. Everything is working well. The provider of the plumbing company are sending emails. Clients are also sending emails and receiving email. Everything is fine.

But one day, Bob accountant receives an urgent email from the manager asking him to download the file and boom. He’s going on a phishing page, and his credentials are compromised, and his email account is compromised and used for spam. What the registrar can do is to completely interrupt the business so the legitimate emails can’t be sent or received. And whereas if you go to the service, the email service provider here, Microsoft, it can operate a surgical strike on the

compromised account. That's for this provider, this email service provider details.

For the hosting provider details, which are helpful for malware, botnet and phishing cases, let's take the case of a charity that registered a domain name and we are hosting a blog on Amazon Web Services, just picking out a random example. And Jane, the volunteer to the charity is a bit behind and she doesn't install the security patches. The blog is compromised and now it's hosting a phishing webpage, which may well be the phishing webpage that was used to hack Bob the accountant from the previous example.

So, what can a registrar do here? It can only suspend the domain name and remove the whole blog of the charity and the email service attached to it so everything will be down. Whereas Amazon, in this example, the hosting company, can remove the compromised pages. So, that's why I think the hosting provider details is also really important.

And third is a regular RDAP that output, which you can already get from the ICANN website or any other registrar website. And you will find ways to contact the registrar. But also, you will also find a way to contact the registrant because even if the WHOIS is now privacy friendly, you still have means to contact the registrant, be it via anonymized email or web form. And that's the first step that any abuse reporter should take. Always contact the registrants. You can also contact the abuse department of the registrar but it's clogging the abuse queue if you haven't contacted the hosting provider, the email service provider or

the registrant first because that's always the first step that the registrar will take. So, that's all for me.

REG LEVY: Thank you, Luc. Sorry for trying to steal your thunder earlier. This one is me. The additional papers that we are currently about to begin work on are coordinating with the Registries Stakeholder Group on a framework for trusted notifiers, a framework that works for registrars as we may have slightly different requirements than a registry operator but we're going to be building on the work that they've already done. And so, hopefully that will be a reasonably easy lift.

Secondarily, we're also going to be building on the registries' excellent work in the IDN homoglyph domain attacks space and looking to see what sorts of things registrars can put into place to help combat that. Next slide, please. And I think I'm going to be turning it back over to Jim now.

JAMES GALVIN: Thank you, Reg Levy. So, thanks to everyone, all of the various registries and registrars. As you can see, I hope all of those who are here are listening. We have quite a crowd here today. There are a lot of registries and registrars, a number of folks who are actively engaged in our work products. And we do appreciate everyone here today and in each of the SOs and ACs who have come forward to talk to us. We are hopefully representing that we are taking on board all of your comments and questions and we are moving forward with actions.

As we move into our discussion opportunity here, just a reminder to folks, the Q and A pod is open. There've been some questions there. We've been answering them. Of course, if you have a question you want to type in the chat room, that's fine too. Now's your opportunity to begin to queue up if you want to speak to us and want to open the discussion by first talking briefly about the definition of DNS abuse.

There's a lot of discussion in the ICANN community at large about what exactly is DNS abuse. Even SSAC noted in its recent publication, SAC115, that there are a number of different definitions that exist within the community at large. This is okay. We accept this, even as registries and registrars. I think this is a good discussion to have about what abuse is and what it can be. This particular definition is important though because it represents the place where registries and registrars all agree that we will act and can act. And in fact, it's embedded in contractual agreements for all of us.

But it's important to understand that this is not everything that registries and registrars respond to. There are many registries and registrars who actually act on other kinds of abuse, too. The DNS abuse framework actually provides different categories of abuse. And we all have our individual terms of service that allow us to perform different actions for different situations. So, but this is the basis really where we focus most of our effort is in these areas and a lot of what we do and what we're doing in our work products is trying to create baseline guidance for how to deal with these forms of abuse and setting up opportunities for folks to continue to act on other things.

So, moving to the next slide, please. We will now open up our general discussion time period and ask for the community here to … These are questions that we have for you and for you to bring any questions or comments that you have for us. We certainly want to hear what you want to ask us about. We'll do our best to answer or perhaps just take those questions on board.

But as we did before, we are certainly interested in how you assess DNS abuse and what it means to you. What are your particular concerns about it? What can you inform us about? And, of course, we really would like to know what we're doing well and what you think we're doing well, especially with respect to all the work products that we've produced, interested in any comments and questions and suggestions you have about that.

And to get us started here, I want to go back to a question that was in the Q and A pod earlier. There was a question from Russ Weinstein about the CPH views on expanding DAAR metrics. Ashley provided a partial response from the registrar perspective and I want to give Samantha Demetriou an opportunity to respond from the registry perspective and ask for other folks, please, to queue up your questions. I'll actually get started here. I'm sorry, Sam. Please go ahead, Sam.

SAMANTHA DEMETRIOU: Thanks so much, Jim. So, as Jim introduced, I'm Samantha Demetriou. I'm the Chair of the Registries Stakeholder Group. And so, in seeing Russ's question, I thought I would offer a bit of background as well for the folks attending this session who may have seen ICANN's blog post

about this topic and might not have all of the relevant details behind it. This is something Jim, at the top of his presentation, mentioned that the Registries Stakeholder Group has been working with ICANN's Office of the CTO staff for a while now on making improvements to the monthly DAAR reports and the data that gets presented through the DAAR system.

I've had some really great exchanges with both Samaneh and with John Crain over on OCTO side. And one of the topics that has come up is the question about integrating registrar data—so, right now, DAAR only reports on registry-level data—whether there was an ability to report on registrar level data in the DAAR outputs. And so, one of the challenges that OCTO has been facing is mapping the domain names to the specific registrar of record.

So, ICANN has approached the registrars about this topic, obviously, as Ashley mentioned in the response to the chat pod but also the Registries Stakeholder Group because in ICANN's view, it would require a slight adjustment to one of the terms of the registry agreement that deals with how bulk registration data access—how that provision is worded to allow ICANN to use that data to do that mapping. And so, similar to what Ashley said about the registrars, it's something that the registries that we're actively discussing and debating right now.

So far, the majority of the responses have been positive in being open to integrating this change into our contracts. There's obviously the question of how to execute that at this point but it's something that we're actively engaged with both ICANN and with our colleagues in the

registrars and the registries about wanting to get done because we think this is … It's a good opportunity for us to continue to sort of push this work forward. So, bit of a long-winded answer, I just wanted to provide the relevant context to folks and happy to take any follow up questions as needed. Thanks, Jim.

JAMES GALVIN: Thank you, Sam. Appreciate that. Brian, did you want to say some more about the—Graeme responded partially in the chat room about the relationship with the PIR Institute and also the I and J relationship questions from the Q and A pod?

BRIAN CIMBOLIC: Sure. Of course. Thanks, Jim. So, yes, so I didn't see Graeme's response, I'm sure. I defer to Graeme on his involvement. But yeah. So, the institute is involved in all of the CPH efforts—sort of works independently but does participate in the CPH abuse groups.

Also, the work of Internet and Jurisdiction, to Peter Van Roste's question in the pod … Yes. I and J has come and presented their toolkits to both of the abuse working groups, the registries and the registrars. Full disclosure, I'm a program coordinator for the domains and jurisdiction contact group. The work of I and J has been really helpful. Some of the work—in particular, the output document from the registries—is based in large part on some of the existing work of Internet and Jurisdiction. So, it's certainly it's been very valuable to both working groups.

And actually just, if I may, since Peter asked the question, Peter, we may be reaching out to you at some point. One of the work groups, the outreach that we want to work closely with is the CC world. So, we'd love to potentially see if there's some overlap between the abuse working groups and CENTR as well.

JAMES GALVIN: Thanks, Brian. Ashley, go ahead, please.

ASHLEY HEINEMAN: Hi. Yeah. Just wanted to expand on Peter's question but also may as well indicate how I responded to Jonathan Zuck's. So, yeah. We've been briefed by both Graeme on the DNS Abuse Institute and we also have had Liz from Internet and Jurisdiction project brief us on the DNS abuse on their efforts on the toolkit.

And as I'm sure most folks know, a number of our members are actively engaged in this effort and the DNS Abuse Institute as they start to engage and we look forward to finding ways that we can collaborate. There's no reason why we shouldn't. We also don't want to find ourselves in the situation of where we're doing the same thing in parallel. So, welcome working with these folks and glad to see that these initiatives are taking off and are doing quite well in terms of deliverables. Thanks.

JAMES GALVIN: Thanks, Ashley. Let me also note, for anyone from ICANN who's here, who's part of this, if there's anyone who would like to offer a response to Fabricio, the question now shows up in the answer section of the Q and A pod. He had a question about abating DNS abuse and ICANN's role in that. If anyone would like to speak to that … I know that Russ is with us. But we would like to offer you that opportunity if you do.

So, thanks to all for the questions. A lot has been going on in the background. I don't know if folks are keeping up with chat room and also keeping up … Oh. I see. So, okay. I'm just getting pointed in the background to Volker. You have your hand up. I just realized I have to look in two places to see the hands. Volker, please go ahead. Or I can ask the folks to give him—

VOLKER GREIMANN: [Inaudible].

JAMES GALVIN: Yes, please go ahead, Volker.

VOLKER GREIMANN: Yes. I just wanted to have one comment with regards to the DNS abuse of registrar scanning with DAAR tool and that only requiring a small change in the registry contract. While in this case, it's probably not a very impactful change, we are usually very concerned about backdooring obligations or requirements or anything that's impactful for registrars through the registry contracts because that's something

that we have no control over. And both parties are basically disinterested in what happens on the registrar level but they could see that as an easy way to get something achieved, easy way to look good, and the work ends up on somebody else's doorstep.

So, this is a practice that has come up more and more often within ICANN that if we can't make registrars do something, we'll just have the registries included in their agreements with the registrars and force them to put in there. And that's, I think, a very concerning development that registrars would like to see ended as soon as possible. If you want us to agree to something, then talk to us. Thank you.

JAMES GALVIN: Thank you, Volker. I see that Ashley has her hand up. Let me turn to Ashley.

ASHLEY HEINEMAN: Thank you. Speaking now primarily as the Registrars Stakeholder Group chair, thank you, Volker, for letting us know your concerns. And as I noted in response to the question, we have not yet had a chance as the full RrSG membership to discuss this in detail. We were given a heads up in advance by Russ that this issue was under consideration at ICANN in terms of a proposal. And I think it's a very interesting concept and I'm actually looking forward to having this conversation but we do need to have it.

There are always going to be concerns that we need to make sure are taken into consideration but I'm also very hopeful that somehow, we

can find a way to participate in this because I think having transparency and being engaged in DAAR, supportive of DAAR is ultimately going to be in our interest but we just have to make sure that it's done in the right way. So, I appreciate your thoughts and concerns and looking forward to having this conversation amongst membership. Thanks.

JAMES GALVIN: Thanks, Ashley. I just wanted to call out for Mason. You got an answer to your question in the Q and A pod but there was also a follow-up question asked to you. If you might want to respond to that, please, and then we'll see if we can get a more complete answer for you. Brian, your hand's up. Go ahead, please.

BRIAN KING: Thanks, Jim. Which Brian?

JAMES GALVIN: Brian King. I'm sorry. And actually what I should ask is, are we on the same topic? If it's a new topic, I'd like to go to Russ Weinstein and give him a chance to respond to the prior questions?

BRIAN KING: Yeah. I'm still on that one, Jim. And my question is probably for Russ so if I could carry on here. It might be a dumb question but Russ, can't ICANN just do a WHOIS lookup and find who the registrar is for the abusive domains? Or if that's a dumb question, sorry, but why do we

need to do anything with a contract or anything? Can't you just look it up?

JAMES GALVIN: So, thanks, Brian King. Let me give a partial technical answer there. It's really about rate limiting and not being able to get the registrar ID out of the RDAP and WHOIS so that's that piece of thing. The other half for your question about contract, I'll leave to Russ to answer. Brian Cimbolic, are you still on topic or can we go to Russ?

BRIAN CIMBOLIC: No, still on topic and actually it might tee up Russ nicely. And my apologies to Brian King. Both Brians had our hands up. And this is not even my registry abuse co-chair capacity but just my own opinion on this is that, the more—we always talk about the principle of subsidiarity, even if we don't use that word. It's the notion—one of the foundations of our discussions on DNS abuse, particularly when we talk about the framework. There's that flowchart that we use pretty routinely and that talks about that abuse should be handled the closest to the abuse that is occurring. And consistent with that is to have DAAR not just mapping at the registry or the TLD level but actually where the registration occurs.

So, I think that having that information available at a registrar level, one, is consistent with the notion of subsidiarity that we've been working on for years. But two, really just, it informs conversation with data. There is currently no DAAR data as it relates to registrars. Having

that information is really helpful and not just speaking to a vacuum or speaking as to smaller subsets of data but having one sort of holistic view of data using the same tool that tracks registry-side abuse. Having that same tool for registrars, I think, would have us in a better position to have informed conversations on abuse moving forward. With that, I think Russ can probably speak to why ICANN's making the request and we can turn it over to you, Russ.

JAMES GALVIN: Thanks, Brian. And, Russ, that was an awful lot of questions and information for you but please, go ahead.

RUSS WEINSTEIN: Thanks everyone. I hope everyone can hear me okay. This is Russ Weinstein from ICANN. So, there were a number of questions in there. Maybe I'll go through them sort of in my own order, in my head here at 1:00 in the morning. I think one of the questions was, what is ICANN's role relating to mitigation of DNS abuse? And I think our role can be summarized fairly succinctly, in that what we believe our role is, is sort of threefold.

One of those is to produce data and analysis to help the community's understanding. And that's where tools like DAAR and the health identifiers, ITHI project, are helpful tools that produce data that the community can use. And we provide additional context to that data to help understand, what is the current situation, what's happening, are

there trends? So, that's one of the reasons, as Brian shared, that we're interested in expanding the DAAR to the registrar level.

Another one of those is to produce tools that help support the mediation of DNS security threats. And an example of this was the DNS sticker project we released last year at the start of the COVID pandemic, where we focus on identifying COVID-related names that are being used for malware and phishing, do some detailed analysis to ensure that there's a high degree of confidence that those names really are being used for malware and phishing, and then provide those to the registrar who can take action. So, that's a tool that enables direct support to mitigating abuse. We've now, as you may have also seen, further expanded that tool. We've enabled the GAC to help provide us new COVID-related search terms that can help broaden the linguistic diversity of the things we look for and notify registrars about.

And then other tools, for example, are the API we have with registries, that we would happily extend to registrars that if we were to include the registrar DAAR data, which provides daily data to the registry about what we're seeing in the DAAR system in their TLDs. So, that's another tool that they have available. And then a third sort of pillar of our role is enforcing the contractual obligations that currently exist today. And so, as you know, we've done previous audits on the registries related to their obligations in spec 11(3)(a) and (b) and right now there's an audit underway regarding the registrars' abuse obligations.

We've also introduced new tools. You've heard about the ERSR tool earlier so that's a tool we have. And also, we've enhanced our

application for registrars to ensure that we're evaluating registrars' competence in assessing DNS abuse and they're understanding their obligations before we accredit them in a more robust way than we were doing previously. So, that's sort of the high-level summary there. Did I answer all the questions involved in that? So, that was the role ICANN plays.

And then there was a question about why do we need the contract change? Brian King, I think you asked that one. I think as, Jim mentioned, it's purely a scale issue. So DAAR is running daily and producing data—reports on a monthly basis but is really providing data to registries daily and doing WHOIS queries at that scale and just doesn't work for either side.

JAMES GALVIN: Thank you, Russ. Appreciate you being able to step up and provide some responses to the question that's going on here. Yeah, I don't think that we should get into the details of trying to solution-solve what's going on with ICANN being able to see a registrar ID or not. That's an open discussion. ICANN and the CPH, we've been very helpful in working together and trying to move forward on that issue. And so, it's best just to let that discussion itself continue and sort itself out.

Coming back to the question from Jonathan Zuck, Jonathan Zuck had early on asked the quantification question in the Q and A pod that I had responded to there in writing and indicated that we, as the CPH, are not taking on quantification task, per se, since others seem to be actively engaged in that activity. But then Jonathan added a follow up question

about without quantification, how do we know which of our efforts are working?

And I want to speak a little bit about that question. I think that it's important to keep in mind that we know as individual registries and registrars, that our efforts are working for those of us who are actively engaged in responding to abuse because we get requests and concerns and reports and we act on those and that's important.

What's interesting to call out about DAAR is, it represents its point in time about abuse. And it is important to keep in mind that there's only some abuse that registries and registrars have complete control over. The vast majority of Internet abuse is not something that registries and registrars control. Bad guys do what bad guys do and abuse comes and goes. So, one of the things that DAAR doesn't show is the churn. It doesn't show the rate at which registries and registrars act on abuse. So, the abuse said, it shows from one month, it might be different abuse from the previous month, even though the numbers are the same. So, it might look like nothing is happening but, in fact, a great deal has happened.

And so, the outstanding work between us and OCTO in particular is about getting a metric that shows the churn—that shows the rate at which registries and registrars are acting. So, that's a level of quantification which would be interesting to the community at large. At least we hope that it would. We think it would be interesting because it more accurately shows that there is activity at least for the abuse that we can deal with and we do deal with all the time. The broader Internet

abuse issues, there are many people who are talking about, that and deal with it, and quantify it, and all of that will continue. And we'll do our best to talk about it and take that on board too.

With respect to the rate limiting, the one issue that I want to add with rate limiting is that, as the story has been told to us, ICANN has explained that they don't want special positioning. So they could query RDAP and WHOIS and get the information about the registrar ID. But in fact, there are no real guidance among registries and registrars about what is proper rate limiting or not. SSAC has reported many times in the past that there are a variety of policies about all of that and ICANN isn't looking for special consideration in getting access to that information from WHOIS and RDAP.

So, that's why we're having this discussion about whether or not there are ultimate solutions that might be more effective for that. And I think that we should just let those discussions continue. We definitely will sort out that problem with them and find a solution that works for all parties, whatever that might entail. So, that's what that is.

I'm looking around. I'm not seeing any other hands up. I'm not seeing any questions. I hope that I answered the rest of Jonathan Zuck's question there about quantification. If no one else has anything that they want to add, I don't see any reason for us to hang out here. Maybe I'll take an opportunity to offer my co-chairs and Ashley and Sam, our stakeholder group chairs, if they have any closing comments. Anybody want to raise their hand and offer a closing comment? Reg, please go ahead.

REG LEVY: Thanks, James, and thank you for moderating this and the answer session as well. Thank you, everybody, for your participation. All of your questions were extremely helpful in terms of focusing our future efforts. And I will turn it back to James or turn it over to Brian.

JAMES GALVIN: Yes. Thank you, Reg. And Brian Cimbolic this time. Go ahead.

BRIAN CIMBOLIC: Yeah. Thanks very much, Jim. Just wanted to say thank you, everyone, for taking the time for joining us. These sessions and our outreach sessions really, more generally, help inform where we spend our time and efforts. So, I'd encourage you. Please reach out to any of the chairs of the abuse groups or the chairs of the broader stakeholder groups if there's an issue that you'd like us to spend our time looking at as it intersects with DNS abuse. You look at almost all of our outputs either stem from or directly tie to some of the discussions we've had with our friends in the various constituencies so just keep it up. The more you let us know where we can be helpful, I think the better the outputs will be for the whole community.

JAMES GALVIN: Thank you, Brian. Ashley?

ASHLEY HEINEMAN: And I'll just quickly jump on that bandwagon and just make sure it's abundantly clear. We want this to be helpful for you. I think we had a realization very recently that we aren't being very good at letting you know what we're doing. So, we're actually trying really hard to change that. I hope that's noticeable. But again, this is important work for us as much as it's important work for you and if there are opportunities where we can get you all engaged earlier, happy to find ways to do that. But thank you all for being here today and I hope it was useful.

JAMES GALVIN: So, thank you all. Thanks to all the participants. Thanks to my co-chairs here. As Ashley said, we very much appreciate this interaction and as Brian and Reg have both added, all of this discussion informs our work and we really do plan to continue to have these as long as we have something to report. We want to open the opportunity for you to come to us. And we will, of course, also continue to meet with the SOs and ACs. So, for those of you who do have opportunities and relationships in those groups, look for those opportunities to come to those joint sessions and we can have more one-on-one discussions and continue to take on work and get your comments and concerns there.

So, I think with that, a reminder. Please fill out the registrar form. Maybe Zoe can post that one last time in the chat room there. Please do fill out their questionnaire, their submission. They're looking for your comments with respect to incentive programs. And I think with that, I will give you back 14 minutes of your day. Thanks all. See you next time.

SUE SCHULER: Thank you. We can end the recording.

[END OF TRANSCRIPTION]