ICANN85 Mumbai | CF – GNSO: DNS Abuse Mitigation PDP1 Working Group Session (3 of 4)
Monday, March 9, 2026 – 13:15 to 14:30 IST

TERRI AGNEW

The recording has started and this is Teri Agnew. Hello and welcome to the DNS Abuse Mitigation PDP-1 Working Group Session 3 of 4. Please note that this session is being recorded and is governed by the ICANN Expected Standard Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct concerning statements of interest.

Please observe the following guidelines to participate in the session. I will also post them in chat for your reference. Only questions posted in Zoom chat identified as a question will be read aloud during the session, as time permits and when directed by the chair of the session. If you wish to speak, please raise your hand in Zoom or otherwise as directed. When speaking, please state your name for the record and speak clearly and at a moderate pace. I will now hand the floor back over to Paul McGrady. Please begin.

PAUL MCGRADY

Thank you, Terri. Thank you, everyone, for being here and as always, we're going to start on time and end on time. So, I appreciate everybody being at their seats. That was great.

This session is a little different from the others. And this session is meant to give us some insight into how the associated domain checks are already being done by some people. The session is not

fulsomely representative of every possible way of doing these associated domain name checks by absolutely everybody in the community that does them.

I actually only a few months ago found out that these were even being done. Because I've sent in a lot of abuse complaints over the years and I've never gotten a response back that said, “And we double checked and here's some other bad stuff you should worry about.” Right? But they’re apparently being done, which is nice and so, part of our process here, we'll bring all that out.

So, the session is intended to inform, but not advocate for any particular way of doing them or not doing them. And it's just to reflect some functions that are already going on in different contexts. So the folks who are going to speak are called SMEs. I want to get out ahead of it. So, if you're like me and you have a lot to learn, SME stands for subject matter expert and I'm here to hear from experts and to learn things.

If you are further along in your journey, then consider the SMEs to be subject matter educators and you can learn what you can and leave behind what you can't. But if you are already an expert, then just think of them as subject matter entertainers. Okay? And try to enjoy yourself as best you can. Okay? All right.

So, while we're pleased to have volunteers from within the working group and appointed speakers representing different business models and stakeholder groups. We did our best to, you know, ensure a bit of diversity and perspective, but, you know, at the

same time, realized we only have a short period of time. We don't have endless hours. We couldn't have everybody here. So, it's, again, not meant to reflect every possible way of doing this.

We want to balance experience with the relevance to the charter questions and so hopefully we hear some folks tying back what they're doing to how the charter questions are written.

We will be making zero decisions and so if you're a decision maker, you've come to the wrong place. We are just listening this time. It's just an opportunity for those of us that are not as far along as some of -- I'm just going to say it. We're not as far along as some of the contracted parties because we don't do these associated domain checks all day long like you guys do. So, we just need to understand it, right?

So, we're pleased to have the speakers and we're grateful for their willingness to do it. They are not being paid so thank you for volunteering your experience and time. And we will have some dedicated discussion time on these inputs. Not today, well, yes, today, but not just today. We will continue to refer back to this session and ask questions about it. So, I don't think I need to slow down. No one's complaining. So please, we're going to go to the next slide.

These are our speakers so if you can, you know, listen, write down the questions and comments, and then we'll have a discussion time. So, I'm going to hand it over to the first and get started. Theo, if you can go first. And then make sure that as each of you SMEs

take your turn, that you, you know, introduce yourself and give a little background about who you are so that folks who don't already know you will have that. So, Theo, go ahead.

THEO GEURTS

Yeah, thanks. My name is Theo Geurts. I'm with Realtime Register. I'm the lead mitigation expert there and when it comes to domain name association, we didn't call it back in the day when I started out a long time ago, and it was basically one of our support tools. It didn't start out as a mitigation tool. It started out as a support tool and that is how we started out when it came to mitigation. So, we've been doing this for quite a while. And I will share my screen here. Let's see where I'm at. Okay, here we go. Excellent.

So basically, when we started out as a mitigation tool, we started to expand on it. Why did we expand on it? Because it made sense to dive deeper into all these associated checks when it comes to criminals so we made a business decision there. And I often hear within the ICANN community that registrars, they always deal with the bottom line. The bottom line is the only thing that's driving them, which is true, by the way, but when stuff makes sense, we are willing to invest.

So, what you see here is a test account. So, anything you're going to see in the sense of criminals, personal data, commercial info, it's all made up and that is for a reason. I don't want to have that exposed so we're doing this on a test account.

So, what you're seeing here is our abuse monitoring system. Why do we have that? Because we want to know which reseller has a large amount of percentage when it comes to criminal activity, phishing, malware, botnets, and so on. Again, this is a test account, so there's not much abuse here. We also invested in monitoring how our customers are doing things when it comes to a whole lot of commercial activity.

Again, this was made for our resellers which are usually hosting companies, so they get a sense on what their customers are doing. And basically, what you see here is where I just check in on a daily basis to see if there are some major shifts here.

If there are major shifts here, then that could indicate it's all legitimate, resellers changing servers, operating systems, which makes sense. But it could also be an indication that there's something up in the sense that there might be criminals that are using a large amount of specific name servers like DDoS Guard.

When we see DDoS Guard as a name server, we go like, hmm, we know those guys, bulletproof hosting services from Russia, let's zoom in there. Anyways, let's get into the meat here and let's zoom in on this domain name.

This domain name was reported by CleanDNS a couple of months ago in January and when we did an associated check, we noticed that this operator was registering crypto drainers. I'm not going to explain that one, and he registered around 60 to 80 domain names

a day. So, he was racking up quite an amount of registrations on a day.

As you can see from this layout here, we don't have much information when it comes to the domain name. We have the domain name, we have when it is registered, we have the name servers, and we have the information about the registrant. That's it.

You can't see any URLs here. If you want to see subdomain names, that is not available on a registrar level. That is available at a DNS level and we provide domain names and we don't provide DNS. We leave that up to our customers.

Our customers are hosting companies, the majority at least, and they provide the DNS. So, if we want to see DNS stuff like subdomain names, you're out of luck here. We can't see that.

What do we know about the registrant? In this case, again, this is all made up. This is Oscar the criminal. We got the address. We got the email address. We got the phone number, zip code, city, and country. These within our system, the way we set this up, and this can vary from registrar to registrar, these are all pivot points, so to speak. The most used pivot point that I use is the email address and sometimes I use the phone number. So, let's put that a little bit into perspective.

We made a little search button here and the moment I use this email address from the registrar it gives me all the domain names

that this person has. So, we suspended around 600 domain names from Oscar and Oscar then changed his behavior. He started not registering 60 domain names. He started to register six domain names to see what happened with those domain names. Apologies.

So, what we did was changing behavior from Oscar and since we did a proactive approach with this criminal here, we would suspend the domain names before they went live. This resulted in the fact that Oscar emailed us that he was very angry with us. We shouldn't take down domain names that weren't engaged in criminal activity so we would have to wait till he committed a crime.

Well, that didn't fly with us so we continued to suspend his domain name. We would check his email address every day, multiple times a day and then at some point, Oscar was gone, which is usually the case.

There's two outcomes here. Usually either the criminals go to a different registrar. That is an outcome that is positive for us because we don't have to do any work. Of course, the cybercrime doesn't stop. It just moves to a different place.

Or, and this is also what we see happen, and this is the exact same thing that happened with Oscar, Oscar started to use different registration data. Every time he would register one domain name,

provide a unique set of registered data, and then register another domain name with a unique set of registered data.

So, there is no association possible on a domain name in combination with the registered data. So, we can still track Oscar. I can't disclose how we do that. It is not based on the domain name anymore in combination with an indicator like email address, but again I cannot disclose it, but most likely they're already criminals attending ICANN meetings, so I don't want to take a chance there.

So, moving on from there, another pivot point is the domain name itself in the sense that we sometimes -- let me sort of explain this. In December, I read an article on the news about peptides. There was an ongoing court case and apparently 58 people died in the Netherlands due to peptides. So, I decided to go like, okay, how many peptide related domain names are there on our platform?

So, this is something we built and it wasn't really easy because if you've got a lot of domain names on your platform, you need to make that you do a lot of database optimization. You also need to do a lot of database security, entry point security so this took quite a while.

So, we can just check on a generic term like peptide, which is here and then we get all the domain names with the word peptide in it. So here we got 24peptides.de. We got bluewellpeptides.com, clearpeptides.com, and so on and so on and so on. So, that is another pivot point that we use to suspend domain names.

How do we suspend domain names? Well, we do it very easily. Let me go here. Domains, Bulk Job, Update Domain Names. Here we put in all the domain names, add a status, Client_Hold, Text, Create Job, Run All Tasks, and we're done. So, bulk is not necessarily a negative term, it can also be used in a positive sense. So, this is basically what I do day to day, all day.

We get many signals from CleanDNS, reporters, victims, law enforcement, Netcraft, so we have this entire process. Let me see how we're doing on time. Cutting it close. One more thing that I want to highlight here. The first time that I suspended domain names in bulk, which is a very long time ago, that caused quite a little bit of issues with our resellers.

When we suspend a domain name, when we inform our reseller why we did it, we provide them with evidence. There's bank phishing, here are screenshots, here is the phishing email, and so on and the reseller goes like, okay, one domain name. When I suspended 5,000 domain names, well, everybody at the reseller was up in arms because how did I dare to touch their beloved customer? They were still thinking in terms of customers, not criminals.

So, when it comes to bulk suspensions, we make sure that everything is on the up and up. We make everything accountable. We make sure there is plenty of evidence. We don't want to end up in a legal team discussion with the reseller that they are going to sue us.

We don't want to be in that position so we always make crystal clear why we've done it and how we have done it. I suspect this will be handy for our discussions later on when it comes to compliance and accountability. That's it from my side.

PAUL MCGRADY: Thank you, Theo. Appreciate that. All right. Next up, we have Natalie Howatson from Com Laude.

NATALIE HOWATSON: Thanks for that, Paul and Theo, great demonstration. So, my name's Natalie Howatson for the record. I work at Com Laude, which is a corporate domain name registrar. As many of you know, there isn't just one type of domain name registrar. There are a few different business models within the space. So, throughout this PDP, I will present from a corporate registrar perspective and our business model operates with a focus on corporate clients instead of the general public.

So, I'll start out with an overview of how you become a client of a corporate registrar, what we define as a client, how a client gains access to a user account to register or edit domains, how we mitigate risk with user accounts, and how we define associated domains across our different types of clients.

So, during this, please keep an open mind when hearing examples of, what works for our registrar business model may not work for other business model types. So to become a corporate registrar

client, you must enter into a contract to be able to access our services and systems. This helps us perform due diligence to mitigate any future risk, such as who can gain access to our internal portal or who is listed as an authorized client contact before we start working on the domain portfolio for any client.

For us as a corporate registrar, we define a client as a corporate entity that we have signed a contract with to provide registrar services. We have two types of clients who we serve within our business model, direct corporate brand clients and reseller clients. A reseller client features one organization managing domains on behalf of various corporate brand clients. And so, they have multiple brand clients within one reseller account.

So up on the screen, just have a little graphic here. We have us as the corporate registrar, our client, and then that breaks down into our two separate kinds of clients. We have the corporate brand client on the left and the reseller client on the right, which contains multiple corporate brand clients within one reseller account.

So, moving on to access our portal, the Com Laude team must create a user account for each individual client user. You don't just automatically have an account. So with this account, the client can view their domains, edit DNS zone files, and change name servers for their domains. When we create new users within our domain portal, we set up varying degrees of permission for each of the client's authorized users.

Not every user has the same type of access, and there are limited contacts per client that have permission to view and access DNS records, zone files, or name servers for the domains in the portfolio. So as described above, included in our client onboarding process, we establish who has the authority to request registrations and make changes to domains. If a request is made by someone who we have not been told has the authority, we follow up and investigate this as a potential security risk.

When we investigate, we are looking for abnormalities. So, for example, if we receive a request by someone who is not authorized to register or audit domains, we speak directly with the main client contract through established channels. This could look different depending on each client. So, some clients, it's a voice call. Other clients, it could be a video call.

When we talk to them, we want to make sure we're speaking to the person who has the authority. And so, for most of our clients, we do have secret passphrases or different types of codes so we can verify that the person on the other end of the phone or video call is that person. We take this approach because this is where the risk is for security issues in our business model.

So, if we turn back to the subject of associated domains, if we define associated as being connected, we as a corporate registrar define an associated domain as a domain that's held within the same corporate brand client account or reseller account.

For example, if we receive an abuse report, that warrants an associated domain check, we will then narrow down which corporate brand client account the domain came from. And we will check various data points like registration logs, what name servers were used, what user registered the domain, if any other domain registrations are suspicious within that same account, as well as speaking with the client directly.

So hopefully this provides more context into how a corporate registrar operates and how we approach associated domain checks. So that's it from me. I'll hand it back over to you, Paul.

PAUL MCGRADY: Thanks, Natalie. Perfect. Perfect on time, too. Love it. We're going to have four and a half minutes now for the other SMEs to ask any questions of Theo or Natalie that they would like. For this first section any hands? Yeah.

VIVEK GOYAL: Natalie, Vivek here from the BC. Thank you for the presentation. You mentioned something and I wanted to get clarity on that, that you consider associated domain to be something which is in the same brand account.

Or if a reseller has multiple brands and the registered domains for multiple brands, but they all belong to the same parent company like, for example, Unilever, right, they have multiple brands and they want to track the brand separately and domain separately for

each brand, would you do associate domain check for all of the brands under the same parent company? Or only for say Dove brand and only check domains registered within the Dove brand account? I hope that made sense?

NATALIE HOWATSON: Yeah, that's a great question. So, for us to expand a bit further, if it was a brand like Unilever, like in your example, we would consider that one corporate client. A reseller would be something more along the lines of, let's say, a law firm. So, they have various distinct corporate brand clients that they manage versus Unilever being the same parent company.

So, within our domain portal, you can have one client brand account and within that brand, they have many different divisions. So, to answer your question, yes, we would find the exact division it was in and inspect that specific division, as well as speaking with the client directly. Hope that answers your question.

VIVEK GOYAL: Yeah. Thank you.

PAUL MCGRADY: Thank you, Natalie. We have a question from Ching and then we will be at time.

CHING CHIAO

Thank you, Paul. This is Ching Chiao from BC. This question is actually for Theo. Theo, once again, thanks for sharing your process. I'm hearing that you're kind of a little bit holding back on talking about bulk suspension. So, I'd just like to get a sense of what would be a process now for bulk, kind of a general, you know, understanding of what you like to do it. You would like to maybe to leave it, for example, for the law enforcement or for the cybersecurity companies to block them, what would be your current practices right now? Thanks.

PAUL MCGRADY

Thanks, and I'm going to intercept this question. We'll have Theo answer it, but we want to keep in mind that what happens after the check is not in our universe, right? But Theo, go ahead, give us a teaser of what life is like out there, but that's outside the scope of our galaxy.

THEO GEURTS

Yeah, sure. So, it just depends on how many domain names are associated and it all deals about risk. It all deals about victims so it can vary from case-to-case basis. You know, the time that we are dealing with botnets, so we were suspending thousands and thousands of domain names, those times are behind us.

But again, we still see lots of domain names associated with what we consider malicious activity, which is sometimes against our service. So this is just a wide variety of reasons, legal requirements

and all kind of stuff that we factor in, which defines maybe something like bulk. I don't know. Thanks.

PAUL MCGRADY: Thank you. All right. We're going to go on to Block B which is going to talk about impacts. And our first SME in Block B is Carlos Becerra.

CARLOS BECERRA: Hey, Paul. Thank you for that and Theo and Natalie, great job. I'm going to tackle the fun topic of impact considerations. Contrary to belief, associated domain name checks are not simply a technical question. It has implications across legal, operational, privacy, human rights, and even competitive dimensions.

A technical association does not equal common control or common intent. For example, shared hosting, reseller, and portfolio environments, unrelated domains often share infrastructure signals. If action is taken based on the association alone, there is risk of over-abroad suspensions, suppression of lawful expression, and economic harm to legitimate registrants, creating a situation where there is guilt simply by association.

This can further be compounded by the sheer volume of requests received and also the sheer volume of incomplete or inadequate reports that a lot of registrants receive. Associated domain name check creates the likelihood of actioning reports that are false positives or create collateral damage.

As infrastructure reuse is common and legitimate, cloud providers, CDN services, corporate portfolios, domain investors, security and testing environments all generate overlapping signals. Shared name servers or IP address and even name commonalities are weak indicators of coordinated abuse. If a policy incentivizes broad sweeps, false positives will increase, leading to business interruption, reputational harm, increased appeals, and potential legal exposure. Accuracy must always outweigh scale.

We must also consider that any associated domain analysis will require access to non-public registrant data, account-level linkage analysis, and internal behavior indicators. This implicates purpose limitation, data minimization, and lawful basis considerations under applicable data protection frameworks.

Actions should be guided what categories of data may be used, what triggers expand review, and what documentation or audit safeguards may apply. Without guide rails, the risk of expanding data processing beyond the purpose for which the data was originally collected increases. And this inevitably leads to the dreaded scope creep, which has different implications depending on registrar business models, as Natalie pointed out. For example, a retail registrar typically has direct contact and relationship, and greater visibility into the end user.

A corporate registrar, as Natalie pointed out, usually controls vetted portfolios with shared infrastructure and centralized configuration as expected. Wholesale or reseller-focused registrars

often have limited visibility into end-user data and operate through layer contractual relationships. There's many more models out there, and we also need to take into consideration the size of the registrars.

Policy demand should recognize the structural differences, visibility, control, and operational capability. We must also consider there isn't headed trade-offs. The broader the view that is required, the slower the response time to clear and present abuse. Careful assessment of operational impact is necessary to develop policy frameworks.

Lastly, but importantly, when associated domain name checks are conducted, there may be an expectation that registrars disclose what additional domain names were reviewed or what linkages were identified. This is simply not feasible. Registrars cannot share non-public registrant data, internal investigative findings, or account-level associations with third parties' absence of a lawful process. Doing so would bring to light data protection concerns, breach of customer confidentiality, and create security risk.

Associated domain analysis, when performed, must remain an internal risk assessment function and not a disclosure mechanism. Happy to take any questions.

PAUL MCGRADY Thanks, Carlos. Appreciate that. I just want you to go back to the very beginning and tell everybody who you're with because I don't know, I think that's helpful. Yeah.

CARLOS BECERRA Yeah. Carlos Becerra. I represent GoDaddy and part of the registrar stakeholders' group. I've been in the industry for about 18, 20 years.

PAUL MCGRADY Perfect. Appreciate that. We have five minutes and 10 seconds for the next little chunk here. And we're supposed to be asking the other SMEs if they have any thoughts on what Carlos had to say, but we sort of broke into, you know, impromptu questions from around the table, which seem fine. And so, any questions or comments for Carlos? I see Gabriel's hands up.

GABRIEL ANDREWS Hi, Carlos. This is Gabriel Andrews, one of the GAC members for the record. And I hear and I take note of many of the important human rights implications that you raised, and they're all valid. I sort of stumbled a little bit when you got to the portion about there being absolutely no data that can be shared as a result of an investigation.

And I wondered if you would disagree that there still is, after an investigation, always an ability to share cybersecurity threat indicators if they don't include information that's PII or Personally

Identifying Information that might otherwise be subjected to dissemination controls or privacy law.

CARLOS BECERRA

Yeah, sure. I mean, definitely we can share some indicators, but I think in practice what we see, at least from my perspective, is the more we share, the more that's expected.

And I think in order for this to be successful, we need to make sure that we set some guide rails as to what data is acceptable to share and not be overreaching.

PAUL MCGRADY

All right. I don't see any other hands so we're reclaiming time fast. This is great. So next up, we're going to hear from Rowena Shue and Graeme Bunton. And you guys, we said five minutes, but we're ahead of schedule so seven to nine. I mean, knock yourself out. Yeah.

GRAEME BUNTON

Luxury. Good afternoon, everyone. My name is Graeme Bunton. I'm the executive director of the NetBeacon Institute. Next slide, please. We'll skip this one because I want to take the most time I can on the substance. Next slide.

NetBeacon Institute, for clarity and to Paul's earlier point about being paid to be here, I'm absolutely paid to be here by Public Interest Registry, who is the parent organization of the NetBeacon

Institute. Although our job is not to carry water for the registry, our job is to try and make the internet safer. One of the ways we do that is running a project to measure abuse across the ecosystem, and that's largely what I'll be drawing on today.

But my goal today is to try and give this group a sense of what abuse looks like across the ecosystem from our perspective, and ultimately to try and help this group get to a place where abuse mitigation happens at the same scale at which abuse occurs.

Next slide, please. Great. So, this is a stacked bar chart of malicious phishing by registrar from, I think it's January 2024 through December 2025. And you can see that abuse is not evenly distributed across the ecosystem. What we see is concentrations of abuse in various registrars, typically in abusive campaigns. And when we think about an associated domain check, at least from our perspective and external perspective, this is often what we're looking to disrupt, mostly, that we're looking to be able to address these large-scale abusive campaigns. So, what does that look like?

Next slide, please. I love these little -- there we go. So, if we do a pretty basic clustering of malicious domains, and malicious phishing only is what we're looking at in this data set, from December and so, we're clustering these domains only on the string similarity. We're not using those tools that Theo was talking about where he's looking at internal data, which registrars might have payment information, customer information, registrant

information, IPS address information, all of that exists only inside of the registrars.

We're looking at this data only from an external perspective and only clustering based on how similar these strings are. Pretty rudimentary, but interesting. And it revealed that approximately 50% of the malicious phishing we saw in December belonged to a campaign in some form. There were 415 where there were five or more domains used, 18 that had about more than 30, and six campaigns of more than 100 domains.

And when we're thinking about how we're addressing abuse, we find that evidencing a campaign, especially the really large ones, effectively at an individual domain level, which is where obligations currently exist, is really difficult to do that at that scale. Next slide, please.

And so, this is an example of what we saw recently in December. There's parking-pcngh.vip. It was an exact replica of a parking fine payment website in the UK. And looking into the data further, we could see, next slide, please, that there were, in fact, 550 domains across two TLDs in this campaign, which really started with parking dash as a prefix.

Registered over a two-week period, give or take, and I should say largely mitigated, that almost all of these domains were at some point suspended. Further in that data, we could see another 68 domains that started with payment dash and another one with

paying dash, all appearing to be of the same sort of UK parking phishing. Next slide, please.

So as one of the questions that was posed in the charter and we've been thinking about is, how do we measure success? If we're looking at these sorts of campaigns, what is going to mean if this associated domain check is working? I think that that's going to mean things like these campaigns get smaller. We see less and less of these thousand, hundreds, thirties plus campaigns because these are discovered easier that they're bad guys registering these campaigns are forced to make them smaller so they're less detectable. We will see them come offline faster and we'll see them come offline more completely.

As I was saying about evidencing individual reports across these campaigns, it's difficult to do that at that scale. An associated domain check will bring them offline more completely. And we'll also see campaigns become centralized, I think, in fewer registrars. We'll see as registrars get better at this across the ecosystem and to me, that's a feature, not a bug. This corralling of abuse, I think, enables compliance to do its work more effectively.

And it also creates an incentive for registrars to be more careful with who they let register larger volumes of domain names. The associated domain check will have some cost and if you have to do that an awful lot, you're going to change how you operate and we think that, again, is a feature. Next slide, please.

And I'll leave you with this one because I think it's come up a little bit and we were asked to sort of think about this and I think we are always at risk of overcomplicating things. And, you know, the ask, I think, from compliance, how do we evidence this sort of work is really, did you do the associated domain check? How did you do it? And what were the results? It's, I think, a pretty straightforward question.

You know, if we're in a place where registrars are lying about their responses to these questions, they can lie to you with the logs as well. That is just an issue that's at play. And I think for registrars to respond effectively to this, it's also pretty simple. In a case like this, it could be, not for a campaign, for an individual abuse report, it could be the report was a single domain. There was no other domains in the customer account. I searched across my domains across these other fields and I came up empty. And that would be, I think, a reasonable answer to that sort of compliance request.

And so, that was the information that I wish to share today. Thank you for allowing us the opportunity.

PAUL MCGRADY All right. Thank you. We got a queue. I'll run the queue. How's that sound? Sarah. Hi.

SARAH WYLD Hi. Sarah Wyld from Tucows. Not a member of this PDP. Just a little question for Graeme about your stacked bar chart. Was the

color in each month the same registrar each month or was it just the most and then so on? Like is blue always the same one? Thank you.

GRAEME BUNTON: Thank you, Sarah, put you in the room and you – okay. Hi, sorry, Graeme from NetBeacon Institute responding to that question, it is the same. It is the same registrar across and we have a blog post from late last year about that, the large blue one is dominant. They had a large abusive campaign mostly toll road phishing in the U.S. that drove that large spike.

PAUL MCGRADY: All right, thank you. Ching Chiao.

CHING CHIAO: Thank you, Chair. Graeme, thanks very much for the presentation. This is Ching from BC. I just need a clarification on the parking ticket sites. Could you maybe elaborate a little bit more, you find those cluster of names, would you be able to identify, for example, through like screenshots for those sites? Or you find, for example, like A records or are they just, follows the same patterns of registration? Thanks.

GRAEME BUNTON: So, on the three examples on that slide of like the payment, parking, et cetera, we had basically the same screenshot for each

one of those so that's how we were able to discern that they were related.

As we turn those into abuse reports, we're capturing things like A records and things like that, but we weren't doing an association that way as we were trying to find that. Like as we're building the clusters, we're really just using string similarity.

PAUL MCGRADY Terrific. All right, my personal favorite, Reg Levy.

REG LEVY Oh, I love you too. Reg Levy, Tucows. I want to clarify that when you said that some registrars are lying --

GRAEME BUNTON No, that's not -- sorry, let me be very clear about that statement. I was not saying that they are lying. I say that if the registrar is lying in their responses, they could be lying in their logs and all those other pieces.

REG LEVY Thank you for that clarification, Reg Levy, again. So, if the implication is that some registrars may be lying and that it is difficult for ICANN compliance to enforce the current policies against lying, liars who lie, what we are doing in this room is not going to solve that issue. So if there are bad actors acting badly, I don't know what we're doing here because we keep putting more

and more onerous requirements on people who are not lying, liars who lie, and the lying liars will continue to lie.

PAUL MCGRADY

Okay. All right. Yeah, so I just want to respond to that if that's okay, which is, yeah. I mean, that's why we're here. Right? I mean, if we only had good actors, we wouldn't be having this PDP. Right? So, I mean, I hear you. Next up is Sarah Wyld again, Sarah Wyld part two, go ahead.

MACIEK PIASECKI

Maciek Piasecki here from EURALO, not part of the PDP, but I'm turning to join as an observer. Thank you for raising your hand for me. So, from what I understood, when you at NetBeacon are able to identify DNS abuse based on the string similarities, you are not using the data that you have, that you're already collecting to do that. So, this would be quite a low-hanging fruit. And I see some efforts to collect even more data from registrants right now at ICANN. Do you think collecting more data would help in the mitigation process that we're trying to achieve here?

GRAEME BUNTON

Thanks. This is Graeme from NetBeacon. So, we collect a bunch of data to measure abuse across the ecosystem. We used source feeds to do that we do quite a bit of work with to try and improve the quality of removed duplicates, remove false positives, work like that. And then we measure where we find domains that are both

live and we believe to be malicious, we turn those into abuse reports and we send them to registrars for mitigation. So, we're taking what we get and we get it to where it needs to go as quickly as we can.

You know, I think more evidence for registrars is always very good. Screenshots, to me, in our data where we're sending abuse reports, are the single biggest factor for mitigation rates. The reports we send that don't include a good quality screenshot often don't get mitigated.

So, pieces of information like that are great. I get nervous when people talk about data because I think often they're then going to go into personal information and registrant data, and I have seen no correlation, and we certainly don't touch it. We don't do anything related to personal information or PII or registrant information. If we're reporting abuse to our registrar, they've already got that information. They certainly don't need it from us.

PAUL MCGRADY Terrific. Thank you. Okay, so that brings to close the official NetBeacon portion of our show and thank you very much. We do still have a couple of people in the queue, and we had time set aside for questions and answers.

So, anybody that wants to ask any question of any of the speakers, go ahead and get in the queue. Those of you with your hands up, if they were questions for NetBeacon, that's perfectly fine, but we

wanted to make sure that everybody knows you could ask a question of anybody. All right. So, we're getting some feedback. All right. Next up is Anil. Go ahead. Anil?

TERRI AGNEW: Anil, your Zoom mic is muted.

ANIL KUMAR JAIN: Yeah. Thank you, Paul. Anil for the record. The question is to Graeme Bunton, two questions. Number one, that over the years since NetBeacon is formed, how much percentage of these abusive domain you are able to reduce? This is number one.

Number two, all these campaigns which you are doing are wonderful, but they are meant, for example, the example you have given about the parking payment, they are directly impacting the public. What is the methodology of informing the public that these domains were malicious and they should be avoiding or what should be the precaution they should take in future to avoid such abuse? Thank you.

GRAEME BUNTON: Thanks. This is Graeme from NetBeacon. I'm a little bit cautious about diving too much into our work in this space. I want to make sure that the PDP is able to do the work it needs to do. I don't know how I would ever answer that first question about what percentage of abuse we were able to reduce.

We help report hundreds of thousands of malicious domain names a year. We see hundreds of thousands of malicious domain names come offline. I have what percentage of that that is of what we've seen, but I don't know how much is out there as a total and so it's a tricky one. And maybe I'm happy to take that offline and have another discussion.

And now I've lost myself on the second question. What was that? Oh, communicating to end users. We publish monthly reports. They're on our website that anybody can go look at. We didn't talk about that specific parking campaign in our most recent report. We do blogs and things like that on abuse issues as we see them.

PAUL MCGRADY Thanks, Graeme. All right. Michael Palage with the bright green shirt. I like it. It's a good look.

MICHAEL PALAGE Thank you, Paul. Go Birds. Michael Palage for the record, speaking in an individual capacity. My question is directed to all of the SMEs associated with the registrar. Could they please explain how they use the unique EPP contact ROID to potentially allocate EPP contact ROIDs to individual clients? And how that can or cannot be used for domain name correlation? Thank you.

PAUL MCGRADY Theo, do you want to handle that for me?

THEO GEURTS Yeah, that's why I raised my hand.

PAUL MCGRADY All right.

THEO GEURTS I sort of expected the question. So, we do use it, but we can't always use it. There are third party modules like WHMS, which even when a contact is unique and even if that contact is being reused over multiple TLDs, multiple registrations, these systems will generate a new contact ID.

So, it isn't efficient, but it is not something we are preventing because we don't want to prevent legitimate third-party modules that are being used worldwide, sometimes are even legacy systems. We don't want to prevent that and we don't see a problem within it when the unique identifier, like an email address, is just as useful. Thanks.

PAUL MCGRADY Thank you. All right. We have Gabriel.

GABRIEL ANDREWS Yeah. Hi, this is Gabriel Andrews again. I had a question for Graeme. Graeme, I think you just said you have, what, hundreds of thousands of domain reports that you issue a year?

Apologies if this is tough to answer in real time, but do you have any sort of feel for how many of those domains are one-offs independent versus how many of those are associated with other domains?

GRAEME BUNTON: Thanks, Gabe. This is Graeme from NetBeacon. It's a tricky question to answer because I haven't done the work to do the clustering across all the months of our data. In the December data from that slide, it's about 50%, from an external perspective is how many I think are registered in multiples. And I think that's probably close-ish. I think it's going to be within 10 either side of that. I would suspect most months unless we're in the middle of that sort of campaign that we saw in March of 25.

PAUL MCGRADY: All right, I see no other hands and I'm going to count down from five, four. Oh, Michael, great. You're back.

MICHAEL PALAGE: Yes. I am back. Michael Palage for the record. So, in response to a lot of the registrars that say they do not assign unique contact ROIDs, that there's basically a contact ROID for each domain name registration, for those that describe that business practice, could they explain how that would be consistent with data minimization that they're always talking about?

Because if you're collecting all of that information, I would like to understand how that is consistent with data minimization. Using one contact ROID across all domain names would seem to be a good approach. There we go. Theo, Reg?

PAUL MCGRADY Thanks, Michael. I'll take back management of the queue. Theo and then Reg.

THEO GEURTS So, strictly speaking for our business here and this is Theo Geurts for the records, we leave that up to our reseller. We don't interfere in their business models and we always say or what we always do is, the reseller is steering this. They are the data controller. If they are doing stuff that doesn't make any sense, they are liable for it.

So, we are not a judge, jury, executioner here. If they want to do it that way, and I agree with you, Michael, it doesn't make a lot of sense. I mean, there's the GDPR. There's all these requirements there. But ultimately, it's the reseller who is doing this and we consider them as the data controller. Thanks.

PAUL MCGRADY Thank you. Reg?

REG LEVY Reg Levy from Tucows. So, the way that our system works is we create a unique ID that we can correlate to a registrant, but that

cannot be associated with registrants by the public and in that way, we minimize data.

PAUL MCGRADY: Terrific. Okay. Any more hands? Any more questions? Great. Well, I'm drawing a line under it then and we will see everybody back here. It's at 3:00 PM local time, right? So, we have a significant break. So, for those of you that did not eat lunch out of Terri's candy stash like I did, feel free to do whatever. I'm going to go grab a sandwich and we'll see you guys back in a little bit. Thank you.

TERRI AGNEW: Thank you. Lisa, you can stop the recording.

[END OF TRANSCRIPTION]