ICANN75 | AGM – Tech Day (3 of 4)
Monday, September 19, 2022 – 15:00 to 16:00 KUL

EBERHARD WOLFGANG LISSE: Jeff Bedser about registry best practices.

JEFFREY BEDSER: Thank you. So I'll just go with the standard good day or bon jour rather than trying to do all the different time zones everyone's covering here, whether you're actually practically in this time zone or somewhere else. I'll be speaking today on registry policy regarding abuse mitigation. So DNS abuse at that level. Next slide, please.

So we're going to be covering in the policy is basically what type of policies you need to have, covering awareness about abuses, efforts, and how to deal with those abuse reports that you receive, and basically how to measure the issues around DNS abuse so that your policy covers everything from what you're going to accept, how you're going to act upon it, and how you're going to measure the outcome of that. Next slide, please.

So under what types of abuse you will address? There's been a lot of conversations over the last several years in the DNS abuse conversations about what is DNS abuse, what is the technical

abuse, etc. And depending on if you're a ccTLD operator, a gTLD, or a registrar, there are different types of abuse you're going to make the decisions on policy-wise that you're going to address or choose to address based on the laws and the regulations that may or may not apply to your business. That can be everything from technical abuse is defined as phishing and malware and such, all the way through to all different types of fraud that can be perpetrated against the people that potentially use the systems that we run.

Then also talking about what constitutes a valid set of evidence for that type of abuse. I think we can all agree that someone's saying, "This is bad, do something about it," really doesn't meet standard for anybody to take an action to basically break a contract. We're talking about a contract with a registrant or a contract between a registrar and a registry. You need to have an evidenced approach to dealing with abuse. So for each type of abuse, what's an acceptable form of evidence for an abuse? For example, on phishing, it might be a screenshot that demonstrates there's an attempt to grab credentials, there could be infrastructure of elements that the IP address has been used or associated with abuse before the name servers, etc. So defining a set of evidence is very important.

Then what actions you'll take. In some registries, they believe that the action component of this is always with the registrar or

sometimes it's with the hosting company, depending on the type of abuse. But based on the type of policy on what type of abuse you're going to address and who's taking the action, is it a suspension of the domain at the registry level? Is it a notice to the registrar to suspend? Or is it simply a notice to the registrant to resolve the issue?

Then lastly, of course, in policy, we need to be talking about the tracking, managing, and reporting, which is really how you retain evidence or how you retain the data. So at a time when someone comes back and says, "This domain had been suspended, why did you do it?" you have a very clear path of this is the evidence, this is when it was reported, this is the action it was requested, and this is when the action was taken. Next slide, please.

Some additional policy points to consider. A registry operator should ensure that the mitigation action is not causing more harm than the abuse alleged reported. And that does come to the term we hear quite a bit about the nuclear option, which is, if the reported abuse is on a domain, let's say it's a compromised domain, and that domain is compromised so it's someone else and it's not the intention of the person who owns the domain to have that abuse occurring on it, that taking the domain out could have commercial consequences to the owner of that domain or other types of harms. So you want to make sure the

mitigating action is relevant to the impact of the abuse reported. For example, if there's child sexual exploitation material on a site that has message boards on it and it has hundreds of thousands of message boards taking the domain down because of that one piece of content may not be the right action. Thousands of records of child sexual exploitation material on a site and then refusing to take them down might be appropriate to take down the whole domain.

Timing, we should intervene immediately when the precision of our action, for example, the serverHold at a registry is justifiable, given either the proven lack of collateral damage that's clearly a malicious or the demonstrable need to disrupt a greater harm. So this does come down to a lot of the conversations that are happening within the community about a malicious registration or compromised domain. If you can demonstrate that the domain is maliciously registered, so it has never done anything good before the reported abuse since it was registered, that's a pretty good indication that domain is maliciously registered. If the domain has been around for a while and maybe even renewed once or twice, and then it became bad is probably a good sign it was compromised. Then considering balancing the policy for the above points—I think I just said that so let me skip to the next slide, please.

So awareness is key, right? So in the gTLD contracts, there's a requirement to have a contact address for abuse. So you're required to have an abuse@ e-mail address. Of course, that is required. The pros are it's very inexpensive to put up an e-mail address and receive e-mail to it. The con is that it's free text. It's somebody explaining what happened to them and entering any words or language they feel necessary to get the point across, and there's not necessarily awareness of your policies or your responsibility to resolve that type of abuse. So while it is a good thing to have, that type of reporting mechanism is not actually the most effective.

There's also Abuse Ingest Forms, much like the one at Net Beacon run by the DNS Abuse Institute, where it's the structure of report that allows someone to put in all the details about the abuse and the supporting evidence, so when it's received by the party that needs to address the abuse to have all the evidence necessary to act upon it. But again, it does rely again on victims to find the form and report it. So it's a limited source of data but it's much easier to work with.

Blocklists are an option. There's quite a bit of use of blocklists in measuring of DNS abuse. For example, DAAR uses Spamhaus and SURBL, which are both blocklist providers. There is a cost associated with it. There's a fee-based model that you will pay,

usually a fee for their data that's equivalent to the domains under management at the registry.

The con is, while they are expensive, they are usually lacking adequate evidence because they're blocklists. They're designed to be used in the browser or at the router level to stop people from going to domains that potentially are bad or have been reported to be bad. So they don't have evidence. So you if you're going to use a blocklist, you need to work out a way to evidence from yourselves under your policy.

Then, of course, there's reporters. Tnd the reporters are basically abuse reporters. They're free because they are usually paid by someone else to find abuses. There's many phish detection providers that are paid by banks and ecommerce platforms to look for phishing domains, and in looking for those domains, they report them with evidence to the providers to get them actions. That doesn't cost you anything, but keep in mind, they're only reporting the ones they've been paid to report to you. It's not necessarily a holistic source or a comprehensive source of abuse on that topic. It just means that someone has found for someone else who's being paid for it.

The last point, of course, here is a hybrid. The best practice for awareness is to do a combination of these things. Find good sources, some of them are free, some of them may be fee setup

models to receive data from many sources. Then basically, you'll have a better chance of getting a more holistic approach to the amount of awareness you can have about the abuse occurring within the zone. Next slide, please.

Effort. This doesn't all happen automatically. So there's going to be someone to review the reports as they come in. This review is going to be does it meet our policy about abuse? Is it evidenced? Does it meet the evidence thresholds to be acted upon? Then there's a relay to the appropriate party for action. Is the person reviewing it have the authority to take an action on it? Or is the person who's taking this report have to relate to someone else to be acted upon? Whether that be a party downstream in the ecosystem such as a registrar hosting company or upstream within the organization such as the general counsel or head of policy is going to take the action?

There needs to be a follow through process. Has the report been actioned appropriately? Once it's received, what's the timeframe? Was it actioned under policy and what are the follow up results on it? Then have the necessary parties been notified about the actions that were taken?

Then finally, tracking. Take the necessary steps to ensure the process of report through notification has been reported to policy so that you can follow through on what was the volume in

the previous period of time, the parties involved, the entities involved, etc. Next slide, please.

Some interesting points of measurements to consider within the policy. Reporting is important to understand the effectiveness of the policy and also the effectiveness of the processes to resolve. So, number of volume of reports received by source. I also like to see from that number of reports actioned under policy, number of reports of domains suspended, number of reports of domains referred to other parties, but also number of false reports. How many reports did we get that were not actionable in our policy or were false? There was actually not an abuse there. The issue with a lot of the abuse@ e-mail, as well as the reporters that are paid, is they will continue to send notices if you're not responding to them. Some of them are known to send up to 15 times a day on the same domain. And if you come back to them and say, "Well, actually, that doesn't meet our policy. We don't act on that," they then submit it under another type of topic saying, "Does it work under this one?" So false reports are very important for establishing trust with your reporters.

Then, basically, number of under-evidenced reports. How many times was it not quite enough? When it was live, it was reported, but the report, by the time you were measuring it to validate it, the domain was no longer up, the content was no longer up so you couldn't take actions, you had no validated evidence of that.

Then, basically, of course, taking all this in a monthly and quarterly and weekly measurement point. So you have an understanding of volumes, impact to organization, etc. I think another interesting point of measurement is looking at correlation between spikes of abuse and spikes of certain types of problems with sales and marketing promotions. When you have a discounted period of time or a volume opportunity, many times you can see increases in abuse correlative to the price. And whether or not you're going to change the policies within the organization about that, understanding that when a certain pricing point hits and that pricing point made a spike in abuse reports, understanding that perhaps there's a correlation there you can work with to determine what is the pricing point that is a good discount for our potential customers but it is not attractive enough to bring in bad actors. Next slide, please.

So then, of course, also measuring by the entities. If you're a registrar, you want to measure by the registrars that the partners that the domain abuse is associated with, and if possible, by registrants. Many times, in a correlative matter, if you pivot on a bad domain and realize it's part of a bulk registration, you can find sometimes hundreds of thousands of other domains in the same pattern that are likely going to be used by abuse and it gives you an opportunity to red flag that abuse or those that may potentially be used in abuse and be

able to react to it more quickly, knowing that that is a correlative point. As I've already made the point, campaign marketing and sales, abuse volume within the incentive programs is really interesting measuring point. Next slide, please, which is my final slide.

Thank you for your time. I'm happy to take any questions.

EBERHARD WOLFGANG LISSE: Thank you very much. Any questions from the floor? We have got Brett Carr.

BRETT CARR: It's not really a question, more a comment and an awareness thing, really. I'm also a member of the ccNSO DNS Abuse Standing Committee. Something we've been working on recently is a survey for ccTLDs to gather information about how they deal with DNS abuse. That survey was released today. So if you're a ccNSO member, we'd really appreciate if you fill it in. Thank you.

EBERHARD WOLFGANG LISSE: I just got it in my e-mail. Anybody else remotely or from the floor? I don't see anyone. Thank you very much. And now Peter Lowe can define DNS abuse for us.

PETER LOWE: I'm not promising that at all. I just want to talk about actually why it's a problem to define DNS abuse, the challenge of defining DNS abuse. Next slide, please.

So I will try not to take up too much time. But I do want to introduce myself to people who don't know me, which I think is pretty much everybody. My name is Peter Lowe. I'm the DNS Abuse Ambassador for FIRST, and I'm the co-chair of the DNS Abuse SIG at FIRST. I worked in DNS security for about three years now, but 28 years in the tech industry. Also I'm the principal security researcher for DNS Filter, and I've been in the tech industry pretty much my whole life. Next slide, please.

If people here aren't familiar with FIRST, it's the Forum of Incident Responders and Security Teams, which I think is a great acronym. But it does make it a little bit hard to google sometimes. Also, it's a bit odd saying that I'm the FIRST DNS Abuse Ambassador. I think, technically, I'm the first FIRST DNS Abuse Ambassador.

The organization was founded in 1990. We enable incident responders to engage with their peers and to foster a shared understanding of security problems. We do that by developing technologies and standards and fostering an environment conducive to their work. It's what it says on their website

anyway. It's just a big organization. Somebody asked me about it yesterday and I said, "It's a kind of like a meta set." I think that's quite a good description. Next slide, please.

DNS abuse as a term. We hear it all the time. I've heard it 20 times today, I think. The problem with it is, it means slightly different things to different people. On the surface, it seems like a simple thing that we all understand. But, actually, it's pretty fuzzy. For a lot of people, it's just malicious domain registration, so domains which are registered for some bad purpose. For other people, it means using the DNS to effective use. Trying to use it for like a C2 domain or something like that. For other people, it's abusing the DNS itself. So trying to do things like DDoS attacks or cache poisoning or something like that. So this means that it's hard to actually define what it means. I don't think there is a very good definition yet. I'll give some examples of those in a second. Next slide, please.

So I went off and had a look at what other people are saying about DNS abuse. Quora—somebody asked and the answer said, "DNS abuse is using some or all parts of a DNS infrastructure to do something it wasn't designed to do." I think that misses the malicious aspect of it and you can have a lot of fun with DNS to make it do things it wasn't designed to do, which maybe aren't actually DNS abuse.

SIDN had a pretty good definition here which was “When people use our DNS servers, there is less server capacity available for others. Excessive use can therefore create problems for everyone else.” So they’re just concerned about abuse of their own DNS service.

The DNS Abuse Institute defines it as “DNS abuse is comprised of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for other forms of DNS abuse).” So they’re focused on I think—well, not narrow, but a fairly specific definition of what DNS abuse covers, which I think has to do with the people who are involved in the DNS Abuse Institute.

I don’t think there’s any real wrong definition. It’s just where people are coming from and what their interests are. Next slide, please.

There was a great article in dotmagazine on this topic on the debate around defining DNS abuse. They wrote, “Domain Name System abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity.” I think this is pretty close to my definition of it, but I have my own biases. I work at a protective DNS service as my day job, and

incident responders have another thing. So this is probably close to my personal definition.

The EU study on Domain Name System. I haven't checked my slides here. I've copied and pasted the same definition twice. Well, the EU study on Domain Name System abuse had a different one. So just pretend there's something slightly different in there.

The ICANN wiki says that "DNS abuse is any malicious activity aimed at disrupting the DNS infrastructure or causing the DNS to operate in an unintended manner." So again, it's slightly different. It's almost the same as the other ones but it's disrupting the DNS infrastructure. This could be DDoS attacks against DNS servers or, again, the DNS to operate in an unintended manner sounds like kind of fun, actually, but that's another topic. Next slide, please.

There's two, I think, main areas when we're talking about DNS abuse which people don't consider often, which is that there is abuse of the DNS and there is abuse via the DNS. There's not as many types that I could think of abuse of the DNS. These are things like cache poisoning, DDoS attacks, and DGA domains. So this is where the DNS is not working as it really should. But then there's lots of abuse that happens via the DNS, and this is where the DNS is actually operating correctly. It's serving up domains

and information about them but it's enabling bad things to happen. So things like C2 domains or phishing, spam and typosquatting are classic examples that a lot of people think of when you mention the term DNS abuse. Next slide, please.

As another example of why it's difficult to nail down what DNS abuse means to everybody. These are just some of the organizations that are out there which focused on it and related to this topic. There's obviously the FIRST DNS Abuse SIG. This is our special interest group at FIRST. I'll talk about that a little bit more in a second. There's the DNS Abuse Institute, the Global Cyber Alliance, ICANN's SSAC and a bunch of other organizations inside ICANN. This is my first ICANN, by the way, so I'm discovering a lot of things about this about ICANN. Shadowserver, Spamhaus, SURBL as well, and a bunch of groups who don't focus on DNS abuse specifically but definitely talk about it. So there's the Messaging Malware Mobile Anti-Abuse Working Group or M3AAWG, their Names and Numbers Committee; KINDNS, who are around here somewhere at the moment; the IETF dnsop Working Group and the RIPE DNS Working Group and APWG. It's Anti-Phishing Working Group. And there's more out there. On the FIRST wiki, we have a list of these. I think when I copied this list from that page, it's since been updated already. I think it was a few days ago. Next slide, please.

The other thing is that there's so many people who are affected by DNS abuse, people who are involved in it, people who are dealing with the effects of it and are affected by it, the people who have to handle the incidents. We have domain registries, the domain registrars, the incident response groups, threat intelligence organizations, governments, enterprise risk management resolvers, so firewalls and filtering services. There's policymakers, law enforcements, rights holders and every single victim of DNS abuse on the Internet. So anybody who's had their website compromised or somebody has been the victim of a phishing attack or even received any phishing, someone who has been using a service which was taken down because of a DDoS attack, this DNS amplification, governments, their law enforcement. There's so many different people who are involved in this or are affected by it. The DNS is such a fundamental part of the Internet that DNS abuse basically applies to everybody. Next slide, please.

So, what can we do about this? It's a fuzzy term but we will use it. It seems like it should be more important that we're all on the same page. I think that it's going to be difficult to achieve. Nobody's going to—well, I don't say nobody—but I don't think we're all going to agree on a common definition. But I think it's important if we try and keep perspective that there are other people coming from a different angle. So you can have your own

definition. But just remember that other people might think something slightly different to you. So when you're using that term, having that awareness that someone else might not have the same understanding is important I think.

One of the things that we're trying to do in the DNS Abuse SIG FIRST is to create a common language. So the different terms that are involved in DNS abuse, we're trying to make it clearer the different types of incidents that that come up and some of the different terms and giving them a definition, and then throwing it out there and seeing how we run. They say the easiest way to find out an answer on the Internet is to say the wrong thing on Twitter and just listen to all the people correcting you. So I think that's something what we're going to try and do.

For myself as the DNS Abuse Ambassador, the FIRST first one, I'm going to try and facilitate conversations and remind people about this and just basically beat the drum, which is what I'm doing right now. Next slide, please.

So I did want to mention a little bit more about the SIG, the Special Interest Group. We're working on providing that common language that I mentioned. We're developing a classification scheme for DNS abuse. So this is where we're going to try and list the different types of DNS abuse incidents,

the stakeholders that are involved, and what you do from the perspective of an incident responder when you're in the middle of an incident that involves DNS abuse. So we want to be able people to say, "Okay, so this is happening, what do I do? Who do I speak to? Who can help? Who's involved?" As a byproduct of that, this is the common language that's being built, and we're having to analyze exactly who is involved, to what degree about, in all the different types of incidents.

We really do have a good representation of different people, organizations, and stakeholders. So we have people from CERTs, Internet governance, commercial resolvers, public resolvers, law enforcement registries, registrars, law enforcement—sorry, missing comma there—registries, registrars, cyber threat intelligence, and other government agencies as well. It's a great group to be part of. I joined and I wasn't even part of FIRST properly at the time, I was just a liaison member, which means that I'm not part of one of the FIRST teams.

We've got people from over 100 countries. The current chairs at the moment are Jonathan Spring from US-CERT. He's also in the ICANN SSAC, I think. He's still active anyway. John Todd from Quad9, and myself from DNS Filter. There's a URL on the screen here if you want to go check it out or you can just go google FIRST DNS abuse. Again, you'll find it. We do have a lot of people

as observers as well. So if you want to come and just check it out, then send us a message get in touch. Next slide, please.

I also wanted to give a little sort of preview of something, this document that we're working on. So this has changed since I took the screenshot, and it's not the whole list of stakeholders. You can see this is what we've been working on for quite some time. It's the second major iteration. We've got a list of all the different incident types that we are looking at. This kind of grew and shrunk a couple of times. But this list has been fairly stable for a while. We're splitting it up into detection via the DNS and mitigation by the DNS as well. So there's another bunch of sheets for that. Then the different stakeholders and to what degree they are involved. So as an incident responder, I can come to this handy-dandy spreadsheet and go, "Right. I am suffering from an on-path DNS attack. Who's going to help me out, the registrars or domain name resellers or whatever?" But as you can see, it does help define the incident types themselves as well. So, hopefully going somewhere to creating that common language.

We're almost ready to share it to the world. There was a previous version that was shared I want to say a year ago. Hopefully I'll be able to give an update on that at some point in the near future, or Jon or someone else. I think I'm pretty much at the end. So next slide, please.

Thanks. I have a horrible Twitter habit. So you can find me on there. LinkedIn or just send me an e-mail and say hi, if you've got any questions or any questions now.

EBERHARD WOLFGANG LISSE: Okay. Thank you very much. Any questions from the floor or remote? Please identify yourself for the record.

PUTERI AMEENA HISHAMMUDDIN: Hi. My name is Puteri Ameena. I'm an ICANN75 Fellow from Malaysia. My question is, as technology evolves, how does the incident responses are changed or updated or adopted to address the abuses? Thank you.

PETER LOWE: Thanks. It's a good question. Well, it's a kind of meta set. So it has certain things from all sorts of different—there's Amazon, there's Akamai cert, there's Microsoft cert, and smaller companies as well. Everybody has their own way of doing things. FIRST itself is just trying to facilitate discussion and connect people together and create this environment to work on things like the DNS Abuse SIG. So I think it depends on who you're working for and how they do it.

EBERHARD WOLFGANG LISSE: To go a little bit deeper, there is also the ccTLDs. gTLDs have a contract with ICANN which specify certain things and which may or may not be enhanced or enlarged in the future to specify other things. ccTLD is generally, with the exception of three or four legacies, do not have such a contract. Especially some quite resolute ccTLD managers who predate ICANN have peculiar meaning about what I think ICANN should do with themselves in this regard. Generally speaking, if there is a relationship, it's bilateral in nature between the ccTLD and between ICANN. So, the subsidiary principle as we call it would require that each ccTLD does what a country basically wants. Because the ccTLD manager is required to reside in that country, it's subject to the local law. So if in Malaysia there is certain restrictions on what content the ccTLD manager is allowed to tolerate, that may be well different from what is happening in Denmark or in Namibia or in the United States. It depends. It's 253 different rules, basically.

Best practice is a good thing. But, for example, in .na, while we do not tolerate really serious abuse, when we see phishing and pharming, we usually speak to the registrar informally. They usually speak to the registrant or the provider informally, and the domain gets either taken off or the website gets cleaned up. But on the other end, these people have paid us to keep the domain registered. If it is clearly fraudulent registration is one

thing. But it's an attack on their system, we can't just take somebody down who has paid us. We have entered into a contractual relationship. We have competition and corruption commission for these things, but they have to go to court for the things. We have indicated to them that we would be a friendly defendant. So if they don't seek a cost against us, we just go watch what they're doing and take the domain of the minute the judge says so. But this is really important. Each country has its own laws and each ccTLD is only subject to those laws and rules and regulations, whether it's industry practice or not. But as Peter says, there is no industry standard. Each company does what they want. So then we had other—sorry, yes?

LEVY SYANSEKE: I'm Levy Syanseke, ICANN75 Fellow from Zambia. I have two questions. Thanks for the presentation. I have two questions. The first one is with regard to DNS, which one is the bigger stakeholder with regard to ensuring security? Does it border more on the user or it comes back to the DNS managers in this case?

Then the second question is you talked about different definitions and you said you had a definition, but I don't think I got your personal definition of DNS abuse.

PETER LOWE: Don't ask me that. That's not fair. Come on. I'm just pointing out the problems. Sorry. Could you repeat the first question, please? Let's focus on that one.

EBERHARD WOLFGANG LISSE: Whose responsibility? Is it the user or the DNS manager?

PETER LOWE: It's a good question. I think there's a shared responsibility to some extent. If you suffer from a crime in real life and you don't report it to the police, it's not your fault that that happened, but you're not helping the situation. But if the police don't do anything about it, that's not helpful either. So I think it's definitely a shared responsibility. But if I had to pick one, I would say probably the people dealing with the DNS abuse, whatever that means.

EBERHARD WOLFGANG LISSE: We have had a hairdresser's website being compromised for phishing, and then we get some ignorant services from overseas telling us we must take the website down. We told them what we think about it and we spoke to the registrar and he cleaned the website up. We speak to the police on a regular basis, they have got a cybercrime unit, and they realize how ignorant they are about these things. They're good at ATM fraud

and they're good at some other stuff, but they're not good at this. They know what fraud is. They're fully aware what they're like. So it's a matter of engagement of the DNS manager of his local law enforcement to build capacity if it were to teach them what can be done, how to do it. As I said, friendly defendant. If they go and make us a participant in a lawsuit, as long as we don't have to pay anyone, we have no real interest. We do what the court says. And that's a simple approach especially for ccTLDs.

PETER LOWE: I'm just going to take a stab at answering the second question, even though I know this is probably going to get me in trouble. I think that DNS abuse is abuse of the DNS or abuse via the DNS and the abuse itself is unintended use of the DNS with malicious intent. I think that's the key part. The malicious intent is the part I would—yeah. Thanks.

EBERHARD WOLFGANG LISSE: I beg to differ a little bit. It's with criminal intent. Malicious intent is probably acceptable under free speech but criminal intent is not. Intent is not proved. But we are all thinking about the same direction, it's just the implementation that differs. Each country has its own.

PETER LOWE: This is a good example of my point that it's hard to define. We've all got slightly different viewpoints. So there was one other person.

EBERHARD WOLFGANG LISSE: Peter Thompson?

PETER THOMPSON: Okay. Let's see if this works. Hi, Peter Thompson. I have a few comments. I hope this is not going to be too long. I do like the efforts of defining DNS abuse. As we found or everybody knows, the term is very much overloaded and it's important to be clear on what is meant in each instance. But I don't agree with the premise that DNS abuse is abuse of the DNS or abuse via the DNS in a very broad sense. I think that is too broad. We need distinction on a higher level.

So here's two examples. If you set up a telephone extension, for example, and then you throw mailings into residential mailboxes and you advertise some fraudulent service, then you wouldn't say that's phonebook abuse, right? It's actually abuse of a phone number assignment. For DNS and malicious registration, I don't think it's DNS abuse, it's a namespace abuse. If our naming system DNS would be replaced by something else, like GNS or whatever, then it would still be abuse of the same namespace. It's actually only randomly or accidentally

connected to the DNS. So I think we should be saying namespace abuse for these malicious registrations and carve that part of the problem out of the term DNS abuse, which simplifies the overloading of the term because you don't have to deal with that anymore.

Then similarly, if you use a phone number to call people for unsolicited marketing, that is spam, right? You wouldn't say it's phonebook abuse. The phonebook is used to find the recipient, right? It's not—

PETER LOWE: That is the DNS working as it's intended, right?

PETER THOMPSON: Right, right, right. So somebody who sets up a domain name under which they run a mail server that sends spam. Yes, that's also in the DNS. But the phonebook is mainly used to find the recipients, not to identify the sending server, which is only accidentally the case. So I think we need a better term for that. I don't know what that term would be. But I also don't think it's DNS abuse.

I think namespace abuse is good for malicious registrations and for technical stuff. I think a broader term like DNS infrastructure abuse or DNS protocol abuse would be good. You have a lot of

suggestions in the table you showed. I don't know if those are meant to be on that level of detail. But I think people in general wouldn't remember all the different distinctions that were like 30 terms or so. So I think we need a high-level distinction of three or four things that we call to be different than the term DNS abuse. And then that narrows down what DNS abuse would be, which is all the rest of that which we can't find a good term.

EBERHARD WOLFGANG LISSE: Okay. I don't want to let this come into a dialogue. I agree that we have a naming issue but it's not helping to refine it into even more complicated names because when I talk to a user or a client, he said, "What? Abuse? DNS? What's that? Website operator, yeah, a company that has a shop on the web." We need to find a name that is short, captures this thing and works with non-technical people. I don't want to continue this any further because we reached the time for the next presentation. We can take this offline if you want. Thank you very much.

Now, Adiel Akplogan will give us an introduction into the new program to promote operational best practices.

ADIEL AKPLOGAN: Thank you, Lisse. This is going to be an overview of this new initiative that we have launched which is KINDNS, you have heard about it. We are very happy, got some good feedback so

far. So I'm going to just introduce you to what KINDNS is, where it comes from, and give you also a very brief overview of our first observation as we have formally launched it as platform since Wednesday last week. Next slide, please.

In one of the previous presentations, there has been a question about how do we measure success of our engagement and capacity building programming and so on. For me, one of the lessons we learned from those activities as well is to be able to collect feedback from people who are running DNS and see what their challenges are. For many of us in this room, we have been interacting with people operating DNS for decades. Yet we see again and again the same mistake, creating same issue, same problem. And getting feedback from the ground is something that we consider as important as well because it allows us to fine tune our engagement but also think about tools that can help you improve the situation because that's our ultimate goal.

KINDNS, the idea behind it is to build a platform and framework that can provide this simple, straightforward information to operators on what are the key critical practices that they have to keep in mind when designing, when developing, and when building their DNS operation platform. If you know and you have been in the DNS landscape for a while, you know that the DNS can be quite complicated. It has a lot of corner cases, it has a lot of specificity. If you know about the Camel Initiative, you know

what I'm talking about. But our goal is to be able to do something that everyone can look at. You don't have to be an expert of the DNS to implement this framework or at least refer to it in how you develop your platform. So it is something that we want to be accessible to any kind of DNS operators, small or big, so we can at least have a common denominator when it comes to a secure operation of the DNS. Next slide, please.

KINDNS stands for Knowledge-sharing and Instantiating Norms for DNS and Naming Security. Well, if you know MANRS, you know what we tried to do there, right? This is pronounced "kindness". So MANRS and KINDNS make the Internet a little bit safer. Next slide, please.

So one of the first work that we did was to look at the different components of the DNS and look at how we can even further slide them to make those norm, those practices, more usable for people who are running the DNS. So, we look at the authoritative server path and the resolver path. For the authoritative, we have split this into two. The first set of practices are applied to TLD managers, but not only TLDs but also critical zone, because we think that the security level should be almost the same if you are running a critical zone or you are running a TLD. Then we have for authoritative, we have the SLD, which is a more generic. Anyone that's running an SLD or even that level can apply those practices.

For the resolver operators, we have three different categories. We have closed and private resolver that you find mostly in corporate network for very specific and limited group of users. We have shared private resolver. They are private but with certain controlled condition to access it. Then we have public resolver that is quite open for anyone to use.

While developing this, one of the discussions we had as well is how do we separate what our core security best practices from pure DNS service best practices. That brought us to create a new cross-cutting category, which is the hardening the core of the system. So you may apply all the DNS core security practice, but if your infrastructure itself is not secure, you may have all of the top best practices but you will still fail. So it's a combination of both operation best practices and system best practices. So we have integrated in KINDNS one category which is cross operators, which is hardening the core of your system.

The other challenge that we put on ourselves is to say, "Well, we don't want for any category to have more than 10 practices." We want this to be simple. We want to really go to the most important and simple and straightforward to implement in most of the case. Each of these categories has maximum eight practices in general, so easy normally for any serious operator to implement.

The goal here is to show, to highlight, to publish those practices, but also to encourage operators to implement them, to adopt them, and join the initiative because it's a framework. And by launching it, it's the starting of the journey. But we want operators to kind of adopt them and show their support in our efforts to make the global DNS a little bit more secure. Next slide, please.

The following slides are mostly the summary of what we have as practices for each of the category that I just mentioned. Starting with the authoritative DNS and critical zone, for instance, DNSSEC is one of the practices that we really think that any serious DNS authoritative server operator should have. KINDNS have that as practice, but KINDNS does not go into the detail about how you sign your zone, how you run your DNSSEC. But it points you to a set of other accessory best practices on how you really run your DNSSEC operation. One of them is the guidebook that we have published in OCTO for ccTLD. That guidebook does not only cover the technical deployment of the DNSSEC but it also covered the administrative part. It covered how you document your system, how you prepare yourself for deploying DNSSEC, etc. So, in KINDNS, what we are asking is that you sign your zone and you deploy DNSSEC.

The second practice, for instance, is that you have to have a good control over how transfer between the authoritative server

is done. You have to make sure that the integrity of your zone is maintaining and constantly controlled. Your authoritative server and your resolvers not run on the same infrastructure. You need to have at least two name servers. You must ensure that you have diversity in the way they operated, diversity from network perspective, from location perspective, and maybe from software perspective as well. You have to monitor your operation. So those are basic simple things that any DNS operator must do. But sometimes people forget some of them or don't see the impact of not doing any of these globally. Next slide, please.

We have the same thing for the SLD operators, seven here instead of eight in the first. Almost the same thing here where we have less emphasis on the diversity part here than we had for the TLD, for instance. So I'm not going to take each of the categories and go in depth in the practice that we are promoting, but that is the concept that KINDNS has. So we can go to the next slide.

So the next slide will be about closed private resolver. Again, there we have validation, which is something that we also have been focusing on in our engagement recently to make sure that that aspect of DNSSEC is also taking into consideration, making sure that you have limited access or restricted access to who your recursive resolver respond to, because this is for closed

private resolver, right? It's not open to anyone. If you are running a private resolver, for instance, you have to provide QNAME minimization to limit leak of private information, privacy information, for instance. Number three, for instance, you won't see it pretty much highlighting in other categories, for instance, but more emphasis on public resolver. You have the separation of infrastructure is here as well. You need to distinct at least the backup for providing your resolver service. Monitoring come back here again. So, as you can see, it is not a set of complex practice here. That has been one of the challenges as well to kind of go down and indentify what is commonly done. Next slide, please.

So, shared private resolver, you have the same thing. Next slide.

Public resolver, same thing. And you can see that for those two, we have DOH and DoT as one of the practice that we are encouraging here for privacy consideration. Next slide.

For the hardening the core, some of them are related to MANRS. Again, you see that there is a complementarity between the two, and other general system security measure that we usually do when we run a public infrastructure in general. We put some emphasis on credential management. You will see it here but you will also see the emphasis on the DNS practice as well. And for those of you who use the self-assessment, you will see that

we have put some emphasis on the credential management as well for people who have a public facing service. Next slide, please.

So, we launched the portal last week. All the practice we just talked about with a little bit more detail. It has a self-assessment tool as well where you can self-assess yourself. All of these are based on voluntary engagement. The self-assessment tool right now is a set of questions where as operator you provide the responses based on how you are running your operation. We don't do any purposive testing or get into your network to test anything. Right now we just rely on what you're saying. Anyway, the report is for you as operator. We are not using the report for anything. It's for you to see where you stand in the DNS in the KINDNS practices and what are the advices we can give to help you improve your DNS practices. So, the report has not only the result of your answer to the survey, but also it points you to a guideline on how you can improve your DNS operation based on the category you have selected.

So the website is kindns.org You can go there. You can look at it and take your self-assessment from. As I mentioned, what we want is for more operators to adopt this. So you can also join as full participant of KINDNS and help us promote and make this more adopted by your operator. Next slide, please.

I've mentioned the self-assessment. It's anonymous. We do not gather any identification on the self-assessment. You can download the self-assessment report if you want at the end of the question. We do have a summary of the responses, though, that give us an idea of what—and I'll share some of the number with you a little bit later on the next slide.

You can enroll into KINDNS. I mean that you give us a little bit more information, though. When you are enrolling to support KINDNS, we ask a little bit more questions than what we ask in the self-assessment report. Basically, why? Because this is voluntary and we want operators to support as much as possible, which means that an operator can decide not to implement one of the practice, but what is important for us is for that operator to explain why not and how they are mitigating the impact of not implementing such practice. So, you can have a way of doing things differently, but still in your overall operation, you are running a secure operation because you know the risk and you are mitigating it in a way. So the enrollment form, when it will be released, now we are doing it manually, ask a little bit more detail. It requires the operator to provide us information about how they are implementing the practice. If not, what they're doing to mitigate the risk.

So, in a week of public operation, we have had more than 200 people who took the survey, that means who took the self-

assessment online. Only 32% of them downloaded the report at the end. You don't need to download the report, because at the end of the report, you have a summary that tells you the scale of your compliance with KINDNS. So I think people, when they see that, they don't feel the need to actually download the survey per se.

Something interesting is that most of the respondents or those who took the survey run both authoritative and recursive resolver, which is quite interesting. The other highlight here is that the majority of people—and that also makes sense—run SLD. So, not TLD managers. You can see on the three other graphs there what are the most popular practice in general. As we all know, DNSSEC is still an issue for many. And in the response for TLD and critical zone, we are still at 51% of people who took the self-assessment that have DNSSEC sign, for instance, for most of the practices.

So, we have this backend information as well, which can also help us fine tune the KINDNS practices in general, but also for us from engagement perspective, that also help us fine tune how we engage with operators and what are the practices on which we can put more emphasis on which we can improve the way we engage with operators in general. Next slide.

So, that's it for KINDNS. You can keep in touch with this initiative, participate, and contribute to it from the different perspective. We have the mailing list that is still up and running. You can join the mailing list and contribute and help us continue to evolve this, to improve it, to make it more mature and accessible to people. The website is up and running. For any questions, you can reach out to us. Reach out via info@kindns.org. Thank you.

EBERHARD WOLFGANG LISSE: Thank you very much. It's quite a good approach to list it in number of minimal standard, the bare minimum that has to be done. I noticed one thing when I went through it. I would propose that on each issue that the self question or whatever identifies, you also put in a link to the documents. For example, the egress BCP and MANRS is not something that I was intrinsically familiar with so I had to Google for it. So if I was you, put on each thing, if somebody is missing, a link on the report that you can click straight, this is where you go and this is where you can read up on it. Are there any questions from the floor?

ADIEL AKPLOGAN: Thank you for that input. In fact, the guidelines are there but we didn't link it. Yes. Thanks.

EBERHARD WOLFGANG LISSE: Calvin?

CALVIN BROWNE: Maybe a suggestion for additional stuff as well. I was looking through some of those very briefly when you had it up on the screen. There were things like having to resolvers on a private organization or something like that, which may or may not be reasonable, depending on certain circumstances. So what I would like to see—and it may still be on the website—because I haven't looked at the reasons for these recommendations, because there needs to be some kind of reasons or some kind of thinking behind these. I mean, you can't just come up with maybe arbitrary standards without having some kind of reasoning behind that. So I'm hoping it's there. And if not, I would suggest that as an enhancement.

EBERHARD WOLFGANG LISSE: This is basically what I just suggested that if you say you have identified you haven't got this, here's the link that you read why you should do this. That's the way I would do it then we have both things together.

CALVIN BROWNE: Yeah. As a link to the technical documentation, which both are valid, yeah.

ADIEL AKPLOGAN: Yeah. Thank you. On the website, you have a plus sign and you have the rationale for each of the practice, which is there already.

The second thing as well is that is the report of how we came up with those practices. The report is not on the website. It's on the wiki, though, because the wiki is the working place where we start working on this. But I think the link to the guideline is something that we will look into to add to the rationale so that it gives people more information. Thank you very much.

EBERHARD WOLFGANG LISSE: There was a remote request.

UNIDENTIFIED FEMALE: Yes. We actually have four questions remotely. We also have a remote participant with their hand raised. What would you like first, Eberhard?

EBERHARD WOLFGANG LISSE: Anyway you like it.

UNIDENTIFIED FEMALE: Okay. Let's take the first question from Levy. "Thank you for the presentation. The approach and the initiative is great. Considering operators have to engage on the initiative voluntarily, how does KINDNS ensure compliance? Lastly, looking at the need for ensuring security and addressing some DNS abuse cases, any plans to share such knowledge with government for adoption in setting policy around DNS abuse in countries?"

ADIEL AKPLOGAN: Good question. The answer is straight. I mean, KINDNS is voluntary. Again, it will be voluntary. We do not plan to force people or enforce it, make it something enforceable. But what we plan to do, though, is to build more and more awareness and capacity building program around KINDNS practices, and make sure that we have enough tools for people to implement them, and encourage people by incentivizing them to implement those practices highlighting the impact. That's also something that we have noticed in our engagement when engaging. People know about the practice but they don't always know the impact of not doing it. That is one of the ways we can incentivize people to be more careful about those practices. But there is no way, as ICANN and as community, I imagine as well for us to make this enforceable. Although it can be something that policymakers,

you mentioned government, can promote well their operators to look into and to encourage them to match their operation to.

EBERHARD WOLFGANG LISSE: Was there another question?

UNIDENTIFIED FEMALE: Yes, we have three more. This one is from Mohamed, a Fellow. "I went through the KINDNS self-assessment. What do you mean by active monitored DNS? Also, is operation diversity meaning using different hardware or software vendors?"

EBERHARD WOLFGANG LISSE: I think that they can ask directly. Next question.

UNIDENTIFIED FEMALE: Next one is "Would surveillance, targeting, and Internet shutdowns mostly backed by governments and corporate institutions on the DNS infrastructure constitute abuse?"

PETER LOWE: Was that a question for me? I started to type out an answer to this but I don't think that there's bandwidth on the Zoom chat to discuss this properly, to be honest. So maybe you could get into

some other way. I'm happy to talk about it. But basically, I think it depends on your point of view.

UNIDENTIFIED FEMALE: Eberhard, the last one is from Hafiz. "How KINDNS is different from NIST STIG for DNS?"

ADIEL AKPLOGAN: The difference here is that, first, KINDNS is meant to be a community-driven initiative. Yet we have in the reference that will list in the KINDNS website, reference to the NIST best practices as well. But as I mentioned, again, we want to streamline the variety of best practices out there, and there are thousands or hundreds of them out there, into something that people can refer to very easily. So this is wider. This is meant to be led by community, but also meant to be simplified so people can adopt it easily.

EBERHARD WOLFGANG LISSE: Last question, Brett Carr.

BRETT CARR: Hi, Adiel. Thank you for this presentation. This has obviously been something that's been going on for a while, and I've been supportive of it since the start. One question I have quickly is, as

part of the MANRS project, they published a list of participants and where they comply with the policies. I wonder if KINDNS apply and do the same thing.

ADIEL AKPLOGAN: Yeah. We plan to do that. There will be a session on participants on the website very soon. We have fine tuning some of the privacy aspect of this before we open it. But it's built in so operators can participate by filling the form and providing us the information. And with their agreement, of course, we will list them with the practice that they're implementing, yes.

EBERHARD WOLFGANG LISSE: Okay. Thank you very much. I think that was a nice session even if we overdrew it a little bit. And for the last block, we see each other in half an hour or in 21 minutes.

[END OF TRANSCRIPTION]