ICANN74 | Policy Forum – At-Large Policy Session 1: Evolving the DNS Abuse Conversation: An end users perspective - The Role of At-Large
Monday, June 13, 2022 – 15:00 to 16:00 AMS

YEŞIM SAĞLAM: Hello, and welcome to At-Large Policy Session, Evolving the DNS Abuse Conversation: An end user's perspective - The Role of At-Large. My name is Yeşim Sağlam, and I am the remote participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior.

During this session, questions and comments submitted in chat will be read aloud if put in the proper form, as noted in the chat. Taking part via audio, if you are remote, please wait until you are called upon and unmute your Zoom microphone. For those of you in the main room, please raise your hand in Zoom and, when called upon, unmute your table microphone. In the secondary room, please raise your hand in Zoom and go to the standalone microphone when called upon.

For the benefit of other participants, please state your name for the record and speak at a reasonable pace. On-site participants may pick up a receiver and use their own headphones to listen to interpretation. Virtual participants may access the interpretation via the Zoom toolbar.

With that, I will hand the floor over to Hadia Elminiawi.

HADIA ELMINIAWI: Thank you so much. Welcome, all, to the At-Large Policy Session on The Role of At-Large and DNS Abuse Mitigation. Malicious activities on the Internet resulting from maliciously-registered domain names and compromised websites threaten the safety of online users. In this session, we are going to focus on the role of the RALOs in organizing the community to help mitigate DNS abuse.

For that, we have a number of panelists who will sort of set the scene for us and guide the discussion. However, we would like this session to be an interactive one, so please feel free to raise your hand and share your thoughts. This is all about the RALOs and what they need to do going forward.

So I'll start with León Sanchez, ICANN Board vice-chair. Welcome, León. And thank you for being with us today. Could you please discuss with us the challenges that the community faces?

LEÓN SÁNCHEZ: Thank you very much, Hadia. First of all, thank you for having me and invited me to this important session. Well, where can I start? Right? The challenges that the community has in terms of DNS abuse are quite a number of challenges.

To begin with, the discussion about how we understand how we define DNS abuse, I think, is the main challenge to begin with. Right? We have some definition in our Bylaws in regards to DNS abuse. We have some guidance as to what can be considered as DNS abuse. But then again, there are conducts and there are situations that might not be as clear-cut, leveled, or considered as DNS abuse or not. So then, again, the challenge is how do we define DNS abuse.

And on top of that, in a different layer but in the same discussion are the different approaches and the different interests that different stakeholders have within this discussion. So I think, again, the main challenge is how do we find a definition or even think if we want to define it. Because maybe defining it will put a tie in our hands for future situations. Right? Maybe we need to think about building in flexibility, in any case, to a definition that comes out from the discussion of the community.

And I think it is also important to highlight that this definition must come from the community and not from the Board or from Org. Right? Because otherwise, it would not be something coming out of our bottom-up multistakeholder decision-making process, and it would be a top-down decision or a top-down imposition.

So that's why I think it is important that, from the Board's point of view, we should be facilitating this discussion. We should be facilitating this dialogue and fostering to create the conditions by which the community is able to discuss what each of the different groups that form our community understands and levels as DNS abuse or not.

And again, to this end there are many efforts. This session is an example of an effort that's being done from within the At-Large community to try to tackle this issue of DNS abuse. There are, of course, other efforts that are being undertaken in the GNSO, in the ccNSO, so on and so forth. So the challenge here, again, is to try to find the right balance and the right inertia or synergy as to form a common understanding of what could be considered as DNS abuse, Hadia.

So again, I think that is the main challenge that we have at hand. And I'm convinced that the Board should play a role as facilitator, as the glue that can bring together the community into a common understanding. But not more than that, at least at this moment.

HADIA ELMINIAWI: Thank you, León, for this. So you mentioned different approaches and different interests. So would this require collaboration? And how do you see us as a community organizing ourselves and working together towards the same goal?

So, there are a number of initiatives all around the community and taken by a lot of the stakeholders. But how can we all work together instead of having initiatives that are going on in parallel?

LEÓN SÁNCHEZ: Thank you, Hadia. I think that one of the strengths that we as a community have is the diversity that lies in it. And as such, I don't see parallel efforts as an obstacle or as a downhill. I think that parallel efforts can lead to a collective effort in the end.

So what I would advise is that we all get involved in each of these parallel efforts and follow that effort and try to feed into the process of that effort. And eventually, I think that all of those efforts will converge in a single track and all the different parallel processes will feed into a single process that could lead us to establish this definition or common understanding of what could be considered as DNS abuse and whatnot.

So again, I think it would be counterproductive for me to say, “Oh, you should do this or you should do that.” No. Again, I think that the richness in our strength is to be able to have these many efforts around a single topic. And then in the end, try to find a way to combine the points of view, the outcome of each of these processes, into more robust and rich wide community effort that can, again, settle this discussion, or at least advance it in a way that can be advantageous to the full community.

HADIA ELMINIAWI: Thank you, León, again. Would you like to briefly mention maybe a point or two in relation to the efforts exerted in that regard?

LEÓN SÁNCHEZ: Do you mean efforts that are being performed by, for example, the community or by ...

HADIA ELMINIAWI: [It could] be the Board or ... Yeah.

LEÓN SÁNCHEZ: Well, the Board is discussing this issue as well. As you mentioned, there are parallel tracks or parallel efforts that are taking place at this moment. And one of those tracks is certainly happening at the Board level. And we recently had a discussion about how to address this challenge of defining or trying to find a common understanding on DNS abuse in our workshop that concluded on Sunday.

So again, this is on top of the Board's mind because we know that it is an important topic not only for the organization, but also for the community. So we are also discussing it.

Now in terms of Org's efforts, I can tell you that there are a number of efforts that Org is undertaking to try to address DNS abuse that vary from the technical point of view to a more pragmatic point of view in facilitating the discussions, in issuing notice of breaches to those who don't comply with the contracts in terms of the DNS abuse provisions, etc.

So, yes, there are a number of efforts that are being undertaken both at the Org and the Board level. And I would definitely invite you to follow them and to feed into the process by touching base with us and letting us know what are your thoughts and your concerns and how we could incorporate your points of view into this effort.

HADIA ELMINIAWI: Thank you so much. We are all looking forward to being part of what you're doing.

So now I go to Joanna. Could you please summarize for us At-Large activities in relation to DNS abuse?

JOANNA KULESZA: Thank you, indeed. And please kindly note I have just been given seven minutes to summarize the rich array of activities that have been happening within the At-Large with regards to DNS abuse.

I echo León's observation that the DNS topic is so persuasive. And it's so broad that it is, on one hand, difficult to address it as a policy topic. But on the other hand, it pops up in whatever policy conversation we might be having. So I'm going to try and highlight it from that angle.

We as the At-Large have identified DNS abuse as a leading topic for the conversations within the community during our previous face-to-face meetings. So it has been a persuasive topic that has accompanied us also throughout the pandemic.

Next to the face-to-face meetings we have organized on DNS abuse during the public forums and during the public meetings we have held, for example in Kobe, with the kind participation from community representatives from other constituencies, Graeme included—thank you again for supporting us always and being here today—we have also held a consistent DNS abuse policy line throughout the pandemic with a set of dedicated initiatives.

Speaking on the outreach and engagement front, we have organized a series of capacity building webinars. That would also be with a sincere thanks to Hadia who was one of the engines behind that initiative, organizing a series of events that would focus on DNS abuse. So we have tried to raise awareness about what DNS abuse might be. This has been done through a series of online meetings. This has also been done through a dedicated ABR that was focused on providing comprehensive information around DNS abuse.

Now because of the pandemic, we were obliged to restrict the number of measures that we could address. But we are very much looking forward to picking up that conversation, particularly with regards to presenting to the broader At-Large community a consistent policy narrative around DNS abuse.

Now this brings me to discuss the policy angle. And indeed, with regards to policy, DNS abuse is an evergreen, ever-present topic. We do have a standing position for DNS abuse within the Consolidated Policy Working Group. And I'm very much looking forward to all of your intervening and providing details on how this has been addressed.

DNS abuse as such, at this point, is not an ICANN policy topic as, for example, the SubPro or Universal Acceptance. Meaning that there isn't an open call for us to provide feedback on. Therefore, we would look into DNS abuse-related issues with the participation of invited speakers or invited guests also from outside the community.

But we would not, or we have thus far not formed a dedicated small working group or small working team that would address DNS abuse as such. It has however popped up in different policy topics, and the At-Large is on the lookout for opportunities to feed the DNS abuse perspective, the end-user perspective, into public consultations and to the process of developing advice and providing advice to the Board.

Now with this in mind, as already said, it is a network of endeavors that we have been engaged in, including working with outside actors—the Internet & Jurisdiction Network included, but not acting as the sole opportunity for us to participate in.

There seems to be forevermore opportunities to discuss DNS abuse also outside the ICANN community. It is a standing topic for a bilateral cooperation between the At-Large and the Governmental Advisory Committee. There is a bilateral small working group that has thus far focused on the European Commission's report that was commissioned by the European Commission for the purpose of analyzing the policy perspectives on DNS abuse. And this small working group has convened a meeting just before ICANN74. We're very much looking forward to that work going on.

So I would highlight these three elements: capacity building, persuasive policy development presence of DNS abuse, and the external networking that has been provided by the At-Large community members. We understand that there is appetite for more, particularly with regards to both raising awareness where DNS abuse does sound very technical and it does require more information to be provided; but also with regards to identifying a very clear and straightforward policy line that the At-Large would be presenting.

As much as we have not identified a need to put together a small working group, that might very well be on the cards. And I defer back to Hadia to take us through this session and see what the opportunities might be.

So these three elements, in my eyes, compose the comprehensive approach that the At-Large has provided with regards to DNS abuse. And I'm very much looking forward to other speakers intervening. Thank you.

HADIA ELMINIAWI: Thank you so much, Joanna. And that opens the door for us to now discuss with the RALOs. We would like to know what's the role of the RALOs and how could they help in mitigating DNS abuse. So I will start with AFRALO. I believe Sean is available with us online. Is he?

SEUN OJEDEJI: Yes. Yes, I'm here.

YEŞIM SAĞLAM: Thank you so much.

SEUN OJEDEJI: Can you hear me?

YEŞIM SAĞLAM: Yeah. Thank you, Sean, for being with us today. So how do you see the role of AFRALO and in helping in DNS abuse mitigation?

SEUN OJEDEJI: I think for us at AFRALO, one thing that is important to note is that our members are actually typical end users who, all they need to do is to go online and see what they want, then click something and have that then produce the expected results that they want. And then they move on.

So we, as AFRALO, I think some of the things that we could do, some of which we have actually been doing also is the outreach and also the capacity building aspect. I think it's very important to note that we do normally run what we call the webinar series, which some of those topics actually circle around DNS abuse as well.

And then occasionally, also, some of our statements. For instance, the statement which we are doing during this ICANN74. Our session that we'll be holding on Wednesday also circles around DNS abuse and what our role could be, generally, as ICANN Board, ICANN community, and of course as AFRALO.

I personally think that awareness and capacity building is the main thing that we as a RALO can do. How do we get these members of ours more aware, more informed in the layman way that actually helps them to better serve the Internet or better utilize the Internet based on some level of layman understanding that they have actually acquired?

But at the same time, as has been noted, there is really no platform within ICANN to contribute to anything related to DNS abuse as such. So when we [build those] capacities or those awareness within AFRALO, as an example, how do we then feed those feedbacks into an existing system within ICANN that would also be good.

So that's why I think that what earlier said in terms of a [inaudible] group could help in this regard so that at least there's an opportunity to actually contribute feedback from the RALOs into that kind of working group. And of course, hopefully certain outcomes would emerge from [inaudible] which can be globally accepted [inaudible] especially with the ICANN context.

So for us as AFRALO, we'll continue to do the outreach. And, of course, we'll continue to do the capacity building, as the case may be. And of course, when the opportunity to contribute into policy-related topics that speaks to DNS abuse, we will continue to encourage our members to do so. Thank you.

YEŞIM SAĞLAM: Thank you, Sean. We have a comment, so I will give the floor to Yeşim. It's in the Zoom chat. Yeşim, please.

YEŞIM SAĞLAM: Thanks so much, Hadia. This is yes Sağlam from ICANN Org. We do have a comment from Naveed Bin Raise. He says, "How I see that DNS Abuse has been accepted by the community is a problem. But we still have no or little consensus among the community about its remit within ICANN. Different parts of communities see different perspective of DNS Abuse. An effort is needed to have a consensus on the community-based definition of DNS Abuse before we can start mitigating the problem." Thank you.

HADIA ELMINIAWI: Thank you so much, Yeşim. So I don't know who would like to comment on this, but my personal view is that we don't need to wait until we reach consensus on the topic in order to start mitigating DNS abuse. Let's start tackling the problem. As Naveed said, we all agree that the problem exists. And that's, in itself, a motivation and a signal for all of us to start looking how to solve this problem.

It is important, indeed, also from an At-Large perspective because it affects Internet and users' safety, and also their trust in one of the organizations, I would say, that has a great weight in the Internet ecosystem, which is ICANN.

So I don't know who would like to comment on this.

JOANNA KULESZA: I'm happy to just briefly chime in. The problem is well noted. We realize that it might not be easy to identify what lies within the scope. But at the same time, it's part of the problem and part of the solution because it's so comprehensive and so broad in its understanding. There is an opportunity for us as the At-Large to reach out to the community and trying to understand what specific aspects of DNS abuse are.

But I would very much look forward to other speakers intervening today, Hadia, where I believe, for example, Graeme might have a very specific answer to that question. Thank you.

GRAEME BUNTON: Hey, all. Thank you. This is Graeme Bunton from the DNS Abuse Institute. I do have thoughts on discussions about definitions. And I actually very much agree with Hadia here, which is that we don't need to come to a place of consensus on a full definition of DNS abuse to make progress. In fact, if I'm going to push pretty hard on this, I think it's very easy to spend lots of time talking about the edges of DNS abuse, and it's actually really hard to make progress and do the work on reducing it.

And so for this community, especially in the context of talking about collaboration, I would say concentrate on those places of agreement and start doing some work on DNS abuse. So we all generally ... No, I don't even think generally. There’s pretty universal agreement that malicious registrations used for phishing, malware, and botnets are DNS abuse and there's work that can be done.

And so for this community, I think—and I’ll talk about this a little bit later in this session—find some opportunities to make some forward progress on those things and put aside these discussions on the edges of DNS abuse because I think they get you very little value.

Lastly, if you really are going to try and dig into definitions of DNS abuse, I think it's folly to try and create a list of specific harms. We use that very frequently as a shorthand in this community because it's convenient and provides some clarity. But I think if you guys really want to tackle that issue, you need to come at an answer that provides a why these particular harms are best mitigated at the DNS. And I think that's really difficult.

So, again, maybe put that aside. Let's look at these places of core consensus and make some progress. Thanks.

HADIA ELMINIAWI: Thank you, Graeme. I move now to APRALO. Satish, could you please tell us how you see the role of APRALO in mitigating DNS abuse?

SATISH BABU: Thanks, Hadia. Thanks for the opportunity. And I know that this is not something that we have discussed a lot in the region, so these are my personal opinions on this subject. And I'm not an expert.

Now they say that security is not a destination, but a journey. And today's DNS abuse, the harms may not be the same over a period of time. So we cannot have a fixed definition. And I find it surprising that we have attempted to define this in the Bylaws which means it makes it very difficult [to kind of ...]

What I would say is that we need a working definition to get started. And then subsequently, as we go forward, GNSO, ccNSO, and the Board should refine this depending on what harm is coming up because this is changing all of the time.

Now regarding what RALOs can do, Sean's already mentioned awareness building/capacity building. These are fundamentals, and I completely agree with him. We need to do it. We may be able to go one step further, advocacy wherein we try to persuade our local organizations/governments to act [whether or not] that they have a role in doing so.

And lastly—fourthly—tools, technologies, and institutions. We heard about NetBeacon. Technologies and things like AI. Can we predict DNS abuse patterns using artificial intelligence? And what are the kinds of institutions we have? Of course, the DNS Abuse Institute. So we can continue to work with them as a RALO.

And finally, the point about the need for a standing group that Joanna had mentioned. I agree, but I may want to propose that we go even beyond. Can we have an inter-RALO DNS abuse watchdog? The reason why I say this is because DNS abuse happens in patterns. You have a natural disaster. You have something in the wake of that. You have an earthquake. You, again, have [inaudible]. You have COVID. You have abuse happening in the wake.

So could we considered a kind of inter-RALO watchdog that keeps track of what's happening in the space? And there may be new threats that are emerging and old threats that are going to get phased out. So it is easier to coordinate action among the At-Large community which is very large and spread out. So, such a thing may be useful to consider.

I'll stop here. Maybe my colleagues would like to add in it. Thank you.

HADIA ELMINIAWI: Thank you, Satish. So indeed, At-Large has the advantage of having a global outreach, and we need to make use of this. I think this is one of the main reasons we are having this conversation today.

Also, you mentioned technology. And I think this is also very important. So far, I don't think At-Large has been using technology much in that regard, either in relation to reporting fraud or maybe tracking.

So I move now to EURALO. I think Olivier is with us online? Yes. Thank you, Olivier, for being with us. So, how do you see EURALO's role? And I know that you are also going to tell us about a tool. Thank you.

OLIVIER CRÉPIN-LEBLOND: Yeah. Thank you very much, Hadia. I hope you can hear me. Is my mic level high enough?

YEŞIM SAĞLAM: We can hear you. Go ahead. Thank you.

OLIVIER CRÉPIN-LEBLOND: Okay, great. Well, you could hear me and just discern my voice. But, okay, I'll speak loud.

So, DNS abuse. It's interesting because we are ... I'm going to take two hats. The first one was, you mentioned earlier regarding to Consolidated Policy Working Group. Actually, Joanna mentioned earlier regarding the Consolidated Policy Working Group. That, indeed, is a group that deals with all policy matters at At-Large. And there are a number of positions that have been established in the Consolidated Policy Working Group. And a number of statements, of course, have been sent to ICANN, in fact, in various different recommendations, and so on.

There's even a dialogue that is now taking place between the ALAC and the Board on some of the responses that were drafted by the Consolidated Policy Working Group and ratified by the ALAC, all regarding DNS abuse. So, it's good to see there is actually an interaction and a dialogue now going on within the Board and our part of the community.

But we still are stuck on this question of how do we actually define it. And when you look at the amount of time we spent on this, it's becoming so academic that, you know, you don't need to define something to actually combat it. And sometimes you all know what it is and the definition might just serve to divide rather than actually to unite people in combating it.

It's interesting because some of our ALSes in EURALO ... And I'm switching hats. One of our At-Large structures in EURALO, ISOC Belgium—the Belgium chapter of the Internet Society—has actually said, "Well, let's forget about the definitions. Let's actually do a tool. Let's do something that will combat DNS abuse."

And they've come up with a thing called isTrust—"Verify the trustability of any website"—because you're dealing here with a domain name and the trust in a domain name to actually depict the actual website of the domain name that it pretends to be, whether it's a brand or something else.

They've come up with a simple add-on for your web browser—and I think it works for Chrome, Firefox, and for Edge—where you just download it and it will give you a little badge in the corner. You can click on that and it will give you the trustability of this website, when the domain was registered, who it belongs to or who was it pertaining to belong to, and what is the communication provider for it.

Check it out. It' called isTrust.org, is the domain that it's under at the moment. And it's just one of the multiple number of things that could be done. This is a free tool with open source that is actually also on the website itself. So you can see it doesn't do anything nasty to you. It doesn't track you around or anything like this. But I think that we should focus a lot on tools. And I'm glad to see, in EURALO, an At-Large structure going in that direction.

With other ALSes around the world having, for many, also a technical remit in some way, maybe we could see more tools like this one to combat DNS abuse rather than trying to find an exact definition, which we'll leave Graeme and his colleagues to work on. Thank you.

YEŞIM SAĞLAM: Thank you, Olivier. So, yes, we need to make use of technology. I know we have a hand in Zoom. Do we, Yeşim?

YEŞIM SAĞLAM: Thank you, Hadia. This is Yeşim Sağlam from ICANN Org. We actually have two hands raised in Zoom. First, Carlos Dionisio. And second, Daniel Nanghaka. Thank you.

HADIA ELMINIAWI: Carlos, please go ahead.

CARLOS DIONISIO: Thank you, Hadia. I believe that Graeme well said, no need of having a definition. I mean, the issue is not having a definition, but installing this topic in the society and recognizing that we have a minimum level of consensus. And that minimal level of consensus is that this is something that is causing us huge harm.

So in order to be able to obtain more voices, to gather more voices—as you said before, Hadia—we do need as many community members as possible and for them to give us their feedback, their opinion on these topics and how they can help us to figure out the solution.

So I believe that we need to work more on spreading the voice and reaching out to other places to create awareness among the community. And not only among us working inside the organization, but we have to even get further away to the academia, to the governmental level.

So I believe that is a huge task that the Institute is already undertaking. And I would like to congratulate you, Graeme, on this great job. And somehow, we're also contributing. Thank you.

HADIA ELMINIAWI: Thank you, Carlos, for your intervention. And now we take the second question.

DANIEL NANGHAKA: Hope you can hear me loud and clear. On issues regarding tackling DNS abuse, I think it takes a different multi-stakeholder approach.

One is the issue over the technical community. The technical community has to make sure that they do appropriate implementation of tools within their respective jurisdictions such that the domain system cannot be abused.

Secondly, when it comes to end user experience, I think we as At-Large have an important role to play. I'd like to say that through outreach and engagement, we have seen a lot of webinars being organized on DNS abuse. We have seen community outreach is going on. We have seen ALSes conducting activities within their respective community when it comes to DNS abuse.

But when it comes to policy implementation, I think also there is the need to bridge the gap on who the exact end users are. What is their uptick when it regards to DNS abuse? So first and foremost, you'll find that end users [just simply] after their website's running, they do not actually understand some of these technologies.

So tools that can be able to test the vulnerability of a website to phishing or spam are very important. And this is whereby we have to preach our gospel louder and louder to the respective end users such that important checkpoints are put forward. If it requires adjusting a policy towards the implementation of DNS abuse in different websites, then that policy would be good, such that it comes from the technical implementation.

As At-Large, we could probably talk to the technical persons, make recommendations to the technical working groups such that it's mandatory for some of these tools to be remitted. It might require an extra cost, but it's better we fight and advocate for a proper stable Internet. Thank you.

YEŞIM SAĞLAM: Thank you so much, Daniel, for your intervention. And now we go to LACRALO. Augusto.

AUGUSTO HO: Thank you very much. I was listening to you all and this search for a unique consensus-based definition on DNS abuse. But at this point in time, I would like to go into details regarding the needs of end users. And that this point in time, I’m not talking only in my capacity of LACRALO chair, but also as an academic professor and lawyer.

In my country, in Panamá, in December there was a bill being passed for each legal person/associations. And as you may understand the entrepreneurship word. That would be a very common term for you all because we know that during the pandemic, many people lost their jobs and many of them started to work in different activities.

So I had been receiving feedback through my students and people from the region, and we understand that these entrepreneurs that are starting in this business area are not the new victims for DNS abuse. They're no longer the large companies and their famous brands, as it was the case in the past.

So let's take into account that we lawyers know when things are not working well. Sometimes we do that for things to work even worse. But this is not the topic today. Entrepreneurs do have .. And this is what we understand. They have a huge amount of ideas and initiatives. And definitely, during the pandemic, they had been the drivers of the economy. So I would like to invite you all to reflect upon this.

And we started detecting among end users in the net those that are really affected. And I believe that this is a sector that is just beginning. And they should be receiving the support of the ideas that we are discussing today.

This morning we said that the DNS abuse is not an abstract topic. I got that idea. And I also took the idea of what we could do. Well, we could start training in terms of DNS abuse reporting. This was a topic that was addressed this morning. I am eager to receive even more feedback to be able to implement further solutions for those that are victims of this DNS abuse. Thank you.

HADIA ELMINIAWI: Thank you so much, Augusto. I like very much your idea about making use of entrepreneurs' ideas to help mitigate DNS abuse. So how do you see, us as At-Large, how can we channel in those ideas—or maybe it's more than ideas—and make use of it?

AUGUSTO HO: I'm going to mention that training is a very important tool for entrepreneurs because entrepreneurs are not only people just starting their businesses. But they're people that are eager to learn. And they represent the new way of economy. And let's be aware that they amount to even 70% or 80% of the economy, together with small- and medium-sized companies.

And definitely, the answer could be training for these people to teach them the techniques available to, for example, fill in an abuse reporting form. Because they are not only losing their ideas, because we also support them in terms of intellectual property. They come with a huge desire to provide support to the worldwide economy. So we are contributing more than we think.

So I believe that there is a certain area of the population where we have to focus our attention because they're also working with ideas. And they're also losing ideas. And they're losing many of the assets that are related to intellectual property because we know the divide in terms of intellectual property and domain names. Thank you.

HADIA ELMINIAWI: Thank you so much, Augusto. We have a hand from León. León, please go ahead.

LEÓN SÁNCHEZ: Thank you very much, Hadia. I think that there is something important to highlight. As Carlos said before and as Graeme said before, if there is something on which we agree, it's that we do not have a definition. And probably, we are not needing a definition on DNS abuse.

However, this does not impede the organization in this case from combatting actively, what we usually know as DNS abuse. And what do I mean by this? Only in 2022, between January and April 2022, the Compliance Department at ICANN started 230 reports related to DNS abuse. So this means that ICANN is not waiting for a general agreement on what we can understand as DNS abuse. ICANN is acting. ICANN is working on the topic in order to be able to not only mitigate but actively combat the DNS abuse.

So, how can this action process be started by ICANN? Well, a good part comes throughout [complaints] that are being submitted by the users. Another part is being started by the proactive monitoring being taken by the organization. And there is another part that comes throughout audits that are being performed to those that are providing services or that are providing domain-related services.

And based on that, ICANN can start sending these notifications to those that are breaching some of the provisions of the agreement, particularly in Section 3.18. And in that sense, the action being taken by ICANN has two stages: an informal stage and a formal stage.

Most of the actions are being solved during the informal stage. Why? Because those that are being notified that might be infringing or that might be unfulfilling the contract have the opportunity to solve the error or to take the necessary actions before sending them a formal notification. And that's why most of the actions end up in this first stage.

Those that are not willing to take actions to remediate the possible failure that may be having terms of compliance with the agreement go to the second stage. And there is a formal action being taken, and there is a more concrete intervention by the organization.

And if, finally, the situation is not corrected, the there are other actions and measures being taken. But what I mean with this is that ICANN is not just waiting for the community to reach consensus. ICANN, with the tools already available and with the definitions already set, is taking actions to mitigate as well as to actively fight against DNS abuse. Thank you.

HADIA ELMINIAWI: Thank you so much, León, for all of this information. So, I have three other hands, but I will go now to NARALO because we are short in time. Eduardo, please go ahead.

EDUARDO DIAZ: Thank you. I'm going to tell you what we are doing within NARALO in order to contribute to mitigating DNS abuse. Basically, this is how we work in the region. At the regional level, we are talking to different representatives of various ALSes and we gather in monthly meetings. We have shared information through DNS-specific webinars for everyone to be aware of DNS abuse.

Of course we can talk about DNS abuse, but sometimes we need to go beyond there. There are some other aspects related to cybersecurity like ransomware that actually are not necessarily to the DNS. But at the ALS level, in my case—in my ALS in Puerto Rico and the Internet Society of Puerto Rico—we have partnered with a very powerful U.S.-based organization, the AARP that is made up of a lot of retired people, people over 50.

And we deliver these webinars to them because, usually, they are the ones who are not aware of these problems. When they receive an e-mail, they don't know whether they should click on the link or not. And when they are looking at a domain, they don't know, actually, what may happen. So we deliver these webinars so they do not fall into the trap of these types of abuse.

Also, we also work with teachers in middle schools. And we also make them aware of how they can protect themselves and how they can protect their information from these kinds of abuses. And other times, we also meet with higher education lecturers so that they are also aware. And in both cases, they can also convey this to the students.

These are the different ways in which we are contributing to mitigating the DNS abuse. It is difficult to measure the results, but we are putting our grain of sand and we are working continuously on this. Thank you.

HADIA ELMINIAWI: Thank you so much, Eduardo. I now go to Graeme. Graeme has a presentation for us. I invite [inaudible], Amrita, and Claire, please put your questions in the chat and we will try to get back to them, even if not during this session. Graeme, please go ahead.

GRAEME BUNTON: Thank you. So working on this theme of collaboration, I've got two pieces I would like to cover for all of you today. The first is that we have launched a service called NetBeacon this week. "We" being the DNS Abuse Institute, which is an organization funded by Public Interest Registry who operate .org. And this initiative is supported by the Institute, PIR, as well as CleanDNS who did the development work for free. And so we're very appreciative of their help here.

So NetBeacon is designed to address two problems. I'll get the next slide, please. And I think we've heard some of this today. Reporting abuse is very difficult. It requires technical knowledge. You need to be able to identify a registrar. You need to be able to find their abuse-reporting function. You need to be able to provide evidence. There's no consistent implementation for these things. And that makes it difficult for end users to report abuse when they encounter it. So that's a real problem.

The other problem is that reports of abuse are brutal. And truly, it's hard to appreciate until you've been on the inside of a registrar and looked at them. The reports that are coming in are unevidenced. They're unactionable. They're duplicative. And they're often not even your domain names.

So registrars and registries are spending huge amounts of time and energy triaging abuse complaints for very little value, for not making the Internet any safer. And it really felt that there was something that could be done to solve both of those problems at the same time. And this is what we've tried to do with NetBeacon. Next slide, please.

So, NetBeacon is a free and easy-to-use site to report abuse. It improves the quality of reports, and it reduces the barriers to action. So the goal there is to make it easy for all of you to report abuse where you've encountered—"you" being end users of the Internet—to report abuse; and make it easy for registrars to receive that abuse, make a determination, and take some action.

Some of the key features of this tool that we've launched are that it standardizes the requirements and formats. It make it pretty easy to report through these relatively easy-to-use forms. We're enriching these reports. So, we take the domain name submitted, the evidence provided by the end user, and we run that domain name through a number of different domain intelligence services and append those results to the report.

The goal there is to move as much of the investigatory burden from the front-line compliance person as we can into the service itself. And then we automatically distribute that report to the appropriate registrar so that end user never has to identify or even understand what a registrar is to submit a report. Next slide, please. Great.

So this is an example of what the form looks like. This is the phishing abuse form. We might have updated some of the text since I made that particular screenshot, but it's pretty straightforward. We're asking for relatively simple information. We've got some reasonable tool tips explaining why and what we're asking for. We allow you to step through it, to save the report and come back to it later if you don't have all of the information handy at that particular moment.

Sorry. I'm just laughing because I realized I used ICANN.org as the example of a phishing domain. Sorry, ICANN. I should change that.

And so you can step through this form and submit abuse. And you don't need to know anything more than what you see there.

There is a little bit of friction to it, I will say. For some users, it's easier just to type an e-mail. But unfortunately, if we want to improve this whole process, forms are the way to do it. And then the other one is that you have to have a verified e-mail address to use the service. Anyone can sign up. You can sign up either using a Google account right now or just creating an account on the service itself. But you have to verify a working e-mail address.

We do not accept anonymous abuse complaints. Those are very difficult for registrars to deal with, especially if they require more information. And abuse reports are frequently weaponized in the industry to attack competitors, to take down websites, to limit speech. And we don't want any of that. So you've got to verify an e-mail address. Next slide, please.

So this is who's supporting the work again. It's the Institute, it's PIR, and it's CleanDNS who have put this together. It's now live. It's now working. As of mid-last week, we've seen really good registrar participation, although registrars don't actually have to sign up because we can send abuse reports to their public e-mail addresses.

And we have a good number of reporters that have signed up and are using it. And I know that domains have gone through it, that we've enriched those abuse reports, that we've sent it to registrars and registrars have taken action. So I feel really good right now that we're beginning to make the Internet a little bit better.

And, boy, I would encourage all of you to try out the tool. If you've encountered abuse, please submit it. And to share this with your communities because I think it's going to be really helpful for reducing DNS abuse across the ecosystem.

So that's one piece I would like to talk about today. And I don't have a ton of time and I know we're running a little bit behind, so I will move on to the second bit I want to talk about, which is really in the spirit of doing work. And that's a thing that is very much central to the DNS Abuse Institute, which is ... Boy, I like talking about abuse, but I like dealing with it and reducing it a whole lot more. And so what I'm trying to give this audience here today is some real concrete action that you can do, some information that you can share that's going to help with abuse.

So at the previous ICANN meeting, there was a pretty fun plenary session that I participated in on the topic of compromised websites versus malicious registrations. And the community got a broader understanding of what that means. And we got a general understanding that we should be treating these different harms separately. So there's still more work to be done on this topic, and you'll see some of this coming out of the Contracted Party House, hopefully in time for the next ICANN meeting in Kuala Lumpur.

But there's a real interesting piece here that I think is important for end users. And if you look at the recent EU study on DNS abuse, you can see that 25% to 41% from that report of DNS abuse is actually compromised websites and not malicious registrations. What I mean by that is that someone was running a website, it got hacked and is now being used for DNS abuse. That 25% for phishing and 41% for malware is a generalization across basically the entire DNS. In some TLDs and some registrars, that percentage is much higher.

So that's a huge percentage. 41% of malware is compromised websites. We can do something about that, and it's very easy to do something about that. And so this is, I think, prime work for ALAC. Next slide, please.

And that is a few very simple things. Practice good password hygiene. Use a password manager. Unique, difficult to guess passwords across all of your services so that things do not get hacked. Enable two-factor authentication your own websites wherever it's available. If you are running a website—if you're operating a small business, whatever it is—enable auto updates on your CMS and your plugins. You've got to keep it up to date. It's part of being a responsible website operator.

Acquire themes and plugins from reputable sources. Often, websites get compromised because they're essentially downloading themes from where they weren't developed and getting a free theme that would normally be a paid theme. But it's coming with malware in it. So be careful about where you acquire your sources.

And then all of you can share these best practices. And in fact, the DNS Abuse Institute published a pretty lengthy blog post that I will paste in the chat that covers a lot of this in some depth. But this work requires sharing. It requires translation so that we can get it to all of the communities who need it.

And that's maybe a good point to end on. NetBeacon right now isn't only in English. We are continuing to shave off some of the rough edges because we've only launched it very recently. But are very aware that it has not been internationalized, and that is on our list of things to do. So we'll get to that, hopefully within the next couple of months, so that the interface is in all of the UN languages to start.

So hopefully those are two real things, concrete things that this community can do to try and reduce DNS abuse. So I'll stop there. Thank you.

HADIA ELMINIAWI: Thank you, Graeme, so much. It's good to know about NetBeacon, this free reporting/DNS abuse website. And also thank you for the tips on how to protect yourself from compromised websites.

We're past our time. Right? Yeah. Thank you so much for being with us today. Apologies because were not able to take all of the questions. We will read the comments and the questions in the chat, and maybe we could discuss them in another At-Large session.

Thank you all, and this session is now closed.

[END OF TRANSCRIPTION]