ICANN83 | PF – GNSO: RrSG-DNS Abuse - Example Review and Panel Discussion
Wednesday, June 11, 2025 – 10:45 to 12:15 CEST

TERRI AGNEW: Hello and welcome to the RrSG DNS Abuse Example Review and Panel Discussion Meeting. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy. If you'd like to speak during the session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom, and on-site participants will use the physical microphone to speak. Helpful hint, if you're in the room, turn off your Zoom audio. Please state your name for the record and speak at a reasonable pace. I will now hand the floor back over to the wonderful Sarah Wyld. Please begin.

SARAH WYLD: Thank you. Am I on? All right. Hello, everybody. Thank you so much for joining us today. This is the Registrar Stakeholder Group's Outreach Team presentation, discussion panel conversation on DNS abuse. So, we try to do a session at each ICANN meeting on a topic of interest. This is the one for today. We hope that this will be interactive and we encourage all of our attendees, as well as panelists, to share their insights and input.

Let's go to the next slide, please. All right. So, what are we doing today? We have invited each group within the ICANN community to share example reports of DNS abuse, and we asked them to provide these example reports exactly as they would submit it to the sponsoring registrar. So, we will be presenting those examples to this group for your consideration. I do want to note that we really appreciate the work from the different groups to provide examples. We probably won't be able to get to all of them today, but we've put them in an order so that we can try to get to one from everybody at least.

The goal here is to understand varying perspectives on how DNS abuse should be addressed. My hope is that we will have a variety of conflicting answers as to what should happen with each one. Because I think that will be more interesting. But we might find that we have converging opinions, and that's also really useful to understand.

Okay, next slide, please. So, thank you so much to our panelists. We really appreciate your participation. I do note that the panelists and the example provider person are not necessarily the same, but we got from each group and thank you for that. They're not sitting in the order listed on screen, but that's okay.

Next, please. Thank you. So how we're going to do this today. First off, we will have a dramatic recitation of the example DNS abuse report. That way, we can all see it on screen, as well as hear it and hopefully process it. As mentioned, we are presenting exactly the

report as it would have been provided to the registrar. That's what we asked for, so that's what we understand that we've received, and that's what we will be displaying here today.

Once the example has been presented, our attendees in the room will be invited through a Zoom poll to indicate what you think the outcome should be for this situation. It might not be the actual final outcome. It might be the first step in a process, but that's what we're asking for is what do you think should happen. And so, we'll talk in a moment about what those options are.

Audience poll happens, and then our panelists will be asked to show what their selection is, or what they think should happen. All the panelists will present their choice, and then two or three people will be asked to speak about it. We'll see how much time we have. Finally, before we reveal, maybe when we reveal the Zoom poll, we will see if any attendees have input to share as well. Any questions so far? We're all with me. We're all happy. We're going to get to that very next.

All right, next slide, please. Before we talk about what the choices are, what is DNS abuse? We have a shared definition. Hooray! So, this is taken from the updated, recently updated Registrar Accreditation Agreement Section 3.18. What are the obligations for registrars? Number one, the registrar shall take reasonable and prompt steps to investigate and respond appropriately to reports of abuse.

What does DNS abuse mean? Malware, botnets, phishing, pharming and spam when it is a delivery mechanism for those other types of abuse. When the registrar has actionable evidence, then they must take the appropriate mitigation actions to stop or otherwise disrupt the name from being used for that abuse. So, those are our parameters here today. We're looking for, does it meet the definition of DNS abuse? And then, what are the reasonable or prompt steps to stop or otherwise disrupt that abuse from happening?

Okay, next slide, please. So, these are the options that we will present to our panelists and to our attendees to select from. You can do outreach. You can maybe contact the reseller, if applicable, or the registrant. Maybe you want to ask for more information. Maybe you want to tell them to do something. That's one option. Another option is to simply make a decision and carry it out. I see this is DNS abuse, and I'm going to do something. I see this is not DNS abuse and I'm not going to do something. This is your decide option.

Third option is to ask for additional information. So, this is going back to the reporter. I wrote "requester" on there because I am just so into registration data disclosures. That is just habit, my fingers type requester, but it means reporter. We're going to ask the reporter for additional information. The fourth option is to look at it yourself as a registrar. Perhaps you look at the website, perhaps you look at the account. Maybe you're pivoting to do additional review. And so, look and see what else is there that we can identify

to then perhaps make a decision. So, that's one of those options that's maybe not the final step, but it's a step on the road.

And finally, maybe you ignore it, maybe you just don't want to answer your emails. We talked about that at the last ICANN meeting. And so, option number five is to ignore the report and do nothing other than an author responder. Any questions? We're all happy. Okay, so moving forward. We will now begin our very first example, and I will ask Reg Levy to please dramatically recite the first example of DNS abuse report. Thank you.

REG LEVY First example from Amnesty International. They are not the domain owner, and the offending domain names are amnestyinternationalantipegasus.com. Sorry, took me a moment to parse that. Amnestyvspegasus.com and antipegasusamnesty.com. There is no applicable email header.

The report says adversaries have set up a phony website that looks like Amnesty International, which is a human rights non-governmental organization.

The attacker-controlled homepage advertises the Amnesty Anti Pegasus software, which the actor is calling AVPegasus, an antivirus tool that claims to protect against the NSO Group's Pegasus tool. However, the download actually installs the little-known Sarwent malware. Sarwent contains the usual abilities of a remote access tool, or RAT, mainly serving as a backdoor on the

victim's machine, and can also activate the remote desktop protocol on the victim's machine, potentially allowing the adversary to access the desktop directly.

We believe this campaign has the potential to infect many users, given the recent spotlight on Amnesty International's groundbreaking report, which is a link on Pegasus spyware. For more information on the incident, please see here, and that is also a link. And I realize I'm speaking quickly. I will try to slow it down in the future.

SARAH WYLD

Thank you, Reg. And if we look at the next slide, you'll see a screenshot of what the reporter included as evidence for the report. For our audience attendee members, there is a Zoom poll up right now, and I will ask our panelists, now is the time. Think about your options, select it, stick it to your paddle, but don't hold it up yet. Attendees, what do you think the registrar should do? Should they outreach to the reseller or registrant, make a decision and just act on it, ask the requester for more information, look for more info, or ignore it and do nothing?

We're going to give everybody a moment. I see votes are coming in. I see panelists are looking through your things. Okay. Does anybody want to identify what type of DNS abuse they think this might represent? All right. How's our poll looking? Should we close the poll? How are our panelists doing? Do we feel ready? All

right. Just a couple more moments so that attendees can continue making their choices. All right.

So, we're closing the poll. And I'm going to ask our panelists, one, two, three, please hold up your responses, for example, one from Amnesty International. Ooh, very good. Okay. So, I see some asking for more information and a bunch of deciding as to what to do next. Very good. Thank you. So, I want to hear from one person who said ask and one person who said decide on our panel as to why you think that's the right course of action. Is anybody very excited to speak first? Volker, please.

VOLKER GREIMANN

Yes. Volker Greimann speaking, Team Internet Group. I think in most cases, this would be an easy decision because there's evidence of impersonation that they're clearly trying to pretend to appear as someone who they are not, with the main purpose of distributing malware. There's sufficient evidence of that malware that is verifiable by us, and there's sufficient evidence presented in form of the screenshots.

However, while the main decision path would be on decide, there may be cases where we would go follow the outreach path because of us being mostly a reseller registrar, we're providing services to a lot of other registrars who have their own abuse processes and who would prefer to make the decision themselves. So, in those cases, we would reach out to those resellers and inform them about the

complaint, forward that complaint and let them make the decision, which we would then verify.

SARAH WYLD: Thank you, Volker. Would any of our panelists who selected "ask" like to speak to why that is your choice? Rida, please go ahead.

RIDA TAHIR: Thank you. I don't have as detailed an answer as my fellow panelist here. I chose to do ask, because this is probably the first time I've looked at a report like this, and I would just ask for more information.

SARAH WYLD: Thank you, Rida. Michaela, did you have something to add to that?

MICHAELA SHAPIRO: Yes, thank you. Now I think this particular situation—and Michaela for the record—just I would want to ensure that the scope of this is quite limited, so that if there were to be any information that Amnesty has posted about their Pegasus report, that there isn't a risk that legitimate websites that are talking about the Pegasus report by Amnesty International are not accidentally taken out as well. So, I think just ensuring that we've covered the correct scope here is important.

SARAH WYLD: Great. Thank you for that, Michaela. Would any of our attendees like to share any thoughts on this example report? I see a hand from Alan Woods.

ALAN WOODS: Thank you. Alan Woods for the record. I think the fact that this is an Amnesty report is a bit of a misnomer. If there is evidence of malware, malware is malware is malware. And therefore, seeking more information of whether or not this is Amnesty or not is probably too much work. We're overcomplicating.

SARAH WYLD: Thank you, yes. And just to clarify, the title on it is simply so that we could identify all of them for the Zoom polls. The title is not-- It's not that Amnesty International reported this to us, necessarily, but yeah. And I see a hand. We're going to go to Jonathan first and then Theo in the Zoom.

JONATHAN ZUCK: Yeah, this is a very interesting exercise. And I guess part of it is, how idealized is it? Because as I'm sitting here thinking about my answer. The fact that it's Amnesty International as the reporter had an effect on me in my decision, just as much as the fact that there was malware there. So, I'm thinking ahead to trusted notifiers or those kinds of things we're talking about. That feels like Amnesty International would find its way on such a list, right? And so that was part of my thinking, although I know that doesn't all exist yet.

So, that's what I meant. It's kind of in an idealized world. An organization like Amnesty International might get some preferential treatment if those kinds of processes were in place.

SARAH WYLD Yes, thank you. That makes sense. And we'll go to Theo, finally. Thank you.

THEO GEURTS Yeah, thanks. So, I'm with Volker. This is easy. But there's also a couple additional steps that can confirm if you're doing the right thing, regardless of the reporter. First, how old is the domain name? That is a major factor. I mean, if it's a couple hours old, okay, there's not much harm in taking it down. Furthermore, if you looked up the domain names like I did in VirusTotal, you get a whole list of antivirus companies that confirm this is malware. So, this is an easy one. Thanks.

SARAH WYLD Thank you, Theo. Can you, Zoe, please put up the Zoom poll results? I'm so sorry, everyone. I got so excited to hear from our attendees that I forgot to put up the Zoom results. So, here's what we see that the attendees suggested. We've got 32% on outreach, 38% on making a decision, 22% asking, 38% on looking for more information. For myself, I think that's where I lie. Someone's telling me it's malware. I want to go get somebody who knows what malware is to look at that before we actually make the

decision. And then 3% said to ignore the report. Does anyone who chose "ignore" want to speak to why that's what they've chosen? Okay. All right. Let us close that one and move on to number two.

REG LEVY

Number two, customer payment request email. Dear Redacted Abuse. This firm represents Redacted and redacted, redacted. Redacted is an alarm and security company serving the redacted areas. Redacted is the name of the former owner of Redacted. It has come to our attention that an unknown registrant registered redacted.com and is sending phishing emails to customers of Redacted. Specifically, these emails are being sent by someone impersonating Redacted, who is the current Front Office Supervisor for Redacted.

In one email, the imposter sends an email to a customer requesting payment of outstanding invoices. As further evidence of this illegal action, the email purports to copy redacted at redacted email address, and includes in Redacted's signature block her first name, the real website for Redacted, and a phone number. A second email, purporting to be from Redacted, seeks payment from another client, falsely claiming payment can only be made via ACH, and volunteering to cover the fees for cancellation of checks that had already been sent to Redacted.

The client reports that they have received five separate notices of these phishing emails. These emails are attached with the headers intact. Pursuant to Section 3.18.2 of the Registrar Accreditation

Agreement, or RRA, we request that Redacted lock the domain name and cease providing services to the registrant to stop its ability to engage in this fraudulent activity. If you need any further information, please do not hesitate to contact me.

SARAH WYLD Thank you for that. If we look to the next slide, it has the sample evidence that was provided and your Zoom poll is up on screen. So, while our attendees are considering what you think should happen, our panelists are making their selections. And I feel like I briefly saw a hand up. No, no hand. Okay. Yeah, all right. Does anyone have questions as we consider what we think should happen in response to this example? No, all right. Are we polling? We are polling. Luc has a question, please.

LUC SEUFER Sorry, I did not catch that. Was there a copy of the email, or it's just an actual copy with the header, or it's just copy pasted inside the body of the email?

SARAH WYLD Good question. Thank you. Let's go back to the previous slide. So, it says header. I know it said header somewhere. Yes, with header. So, we can, I think, accept that headers are not just pasted in, but actually included as appropriate evidence. All right, so we will go to our panelists. What do we think should happen for this one? We don't have to close the poll. Do we have to close the poll? Don't

cheat on the poll. Make your own decision. Don't be influenced by the panel. All right, we're ending the poll. I see a decide, look, ask, outreach, ask, decide. This is great. Okay. I want to hear from two people who haven't spoken yet. Jeff, please go ahead. What do you think?

JEFF BEDSER: So, I think this is where Luc was going, but that's not the headers that are necessary to determine the sender. That's the headers that can be spoofed. We need the full headers to make a determination. So, I'd have to respond and ask for more details, the actual headers of the email that demonstrate those domains were used to send the email.

SARAH WYLD: Thank you, Jeff. And would any of our other panelists who selected decide like to speak to that? Thanks, John.

JOHN MCELWAINE: So, this was my example. The actual emails, so the intact emails were provided in this particular case. I actually received it from the client who had received it from the customer. So, that was provided. And again, I thought this was a pretty clear-cut case of phishing and had all the right evidence.

SARAH WYLD Thank you very much. Would any of our other panelists like to weigh in here? Volker, thank you.

VOLKER GREIMANN Yes. I chose look, but with a very heavy slant towards decide, because looking would just be basically confirming my already made decision. I would have a look at the registration date. Is this a new domain name? And at the registration data that we have available in that domain name. If there were information in that data that indicated that this could be a legitimate registration, I would then ask if they were certain. Because we have had cases where other companies were flagging emails from subsidiaries as phishing, because subsidiaries were sending those out and one hand didn't know what the other was doing. But if this was, which is mostly the case, John Smith at whatever, registering that domain name, that would be an instant takedown.

SARAH WYLD Thank you, Volker. So, we will now reveal the results of our attendee poll. Oh, so we've got a lot of people saying decide. It's phishing and we're done with it. We see some outreach, we see some ask, some look, and again some ignore and do nothing. Thank you to Luc for sharing in the Zoom chat. There is a link to how to get the email headers to then include in an abuse report. We hope that that is a helpful resource. Would any of our attendees

like to speak to their selection or what they think should happen? Michele, please go ahead.

MICHELE NEYLON: Yeah, thanks. Michele for the record. I'm a House fan. Remember the TV show? Everybody lies. There's no way for us to know unless we look at the website, the email, the headers and everything. There's no way for us to know that the report we've been given is actually true. We can't assume. If it's my client who's sending me the report, I have information about them, so I'm going to have a different approach. And I can understand why you would take your client's report that way. That makes perfect sense to me.

I don't have that relationship. I have no way of knowing who the hell they are, so I'm going to have to look at it more closely. This kind of attack we have seen quite a bit of, and we've seen variants of it, and it's nasty and it's quite awkward. And often it involves registrars who don't respond to things, and it's a pain. We've had a bunch of these involving things. But the thing about the subsidiaries is also really, really frustrating, the right hand not knowing what the left hand is doing. We've had these that happen multiple times as well.

SARAH WYLD: Thank you, Michele. I see a hand up from Owen.

OWEN SMIGELSKI

Thanks, Sarah. Owen Smigelski for the transcript. So, I was similar to Volker where I was 90% decide but ask was that little 10%. And that's just to check to see how new the domain name is, what's in the account, what are the other domains that they have. Are they doing similar things? This seems like a very classic BEC, business email compromise, type phishing campaign we see a lot and more often than not, it's something completely illegitimate.

I know there can be sometimes where you have competing divisions of corporations that have registrations across different registrars or resellers that might be doing that. But this seems to be a very small business here, where I doubt that that's coming into it. So, I'm leaning a lot more toward I didn't have the check, but then decide, but it seemed like it was pretty much a clear cut. Shut it down. Thanks.

SARAH WYLD

Thank you, Owen. Would anybody else like to speak to this example where they see-- Oh, yes, Michaela. Thank you,

MICHAELA SHAPIRO

No, I just wanted to jump in to say, because I think my concern in this particular scenario was the request to lock the domain name. And again, I'm not a registrar, so I can't speak on that issue, but what I can say is from the perspective of the registrant. As similar to what Michele said, I would want to ensure that this is-- I want more information. I want to understand, and I would actually want

to do outreach to the registrant before blocking or before locking the domains.

So, I was between ask and outreach, and look. I wanted more information before any action is taken, which is quite extreme in some cases, and it could be valid in this case. If it is as clear cut as it looks to be, I would be very supportive of locking it, but I would want to do the outreach to the registrant first.

OWEN SMIGELSKI: But thanks for that feedback. Just to add from a registrar perspective. In Namecheap, we get hundreds of thousands of these abuse complaints every year. And if you follow up with every single customer asking them, that just adds in a delay in a process. And if this is somebody sending out 20 of these emails a day, that be concerned. So, normally we do is suspend, but they have a way, a recourse to come back. Let's say we suspended it. Oh, you can do this to improve it. Sometimes they come back, most of the time they don't, other times they just try and transfer out and then complain to ICANN that we lock their domain name and they can't transfer to another registrar.

MICHAELA SHAPIRO: Yeah, no, just to say, and I think that's hard in these scenarios without having information about the processes involved. So, I really appreciate that. That's great to hear that transparency and access to remedy is there. So, thank you.

REG LEVY

Reg Levy from Tucows. And we also get hundreds of thousands of these a year, and we do follow up. So, our impulse is not suspend at the first instance. We typically reach out to the various parties involved.

ALAN WOODS

Alan Woods for the record. Just a point of clarification on this. I think everybody's mind looking at these is probably going to the fact, well, obviously I'm going to verify this. So, I think just for ease, if we say yes, obviously you're going to. Before you decide, you will take some verification action, whether or not it is to verify that it is correct or verify that it is incorrect. So, I just might make things a little easier because we all think, well, I'm going to look at it first and verify it.

SARAH WYLD

Thank you, Alan. All right. Any final thoughts before we move on to our third example? Yes, Marc, please, and Volker, and then we'll go on.

MARC TRACHTENBERG

Marc Trachtenberg for the record. This seems to be a really easy case. As John said, he submitted the actual emails, not a copy and paste, not a PDF. The email messages themselves, where it's very easy to view the headers for anyone here who's at a registry or

registrar that has any sort of basic technical expertise. So, this is a no-brainer. I don't understand why anyone would be reaching out to the registrant for more information. You have a report. It's a lookalike domain name. It's not going to be a subsidiary who registered the lookalike domain name. You have the phishing emails. You're overcomplicating it, making it too hard. There's a lot of other great area cases where you probably want to do some research and you want to check it out. This is not one.

SARAH WYLD Thank you, Marc. I think part of the unclarity might have been that in the screenshots that we provided, it wasn't super clear that the headers were actually included in the report, but they would have been.

MARC TRACHTENBERG But John clarified that he submitted the actual email messages as attachments, so they would be available.

SARAH WYLD They would indeed be available, yes. I see Jeff wants to respond, and then we'll go to Volker.

JEFF BEDSER Over a career, I've seen many times where people are deceptive and reporting harms to get someone else's business interfered with. Any header is text. Any text can be edited by a text editor. So,

you have to verify, because you're basically taking this customer's word on the fact that this happened without verification is literally giving the opportunity for them to abuse another company.

The number of times I've seen these in the exact scenario where two competitors are reporting each other in this scenario saying they're causing a harm and it's not there. It's just someone trying to interfere with another business to get their website taken down. So, you have to be careful because that's that interference. And that's also why they keep pointing out to the age of the domain is important because the domain is more than a year old, it's more likely to be used very legitimately, up to the point where it's been reported. And then doing a suspension immediately is a very opportunity to break a contract where there are going to be legal consequences that we don't want to have to deal with. So, the age of the domain is important as well.

MARC TRACHTENBERG: But again, that is not possible here. The actual email messages were attached so someone could not have gone in and used a text editor to change the headers. You have the messages where you can check the headers in the message itself.

JEFF BEDSER: But Marc, you don't know that from the example.

MARC TRACHTENBERG He said it.

JEFF BEDSER I understand that, but we voted before he said that.

MARC TRACHTENBERG Right, but you're taking the comment now, after having the information and so everyone's still going back to the same thing after. I agree it was somewhat ambiguous in the example on the slide, but now, at this point, we have the information. He said it. I repeated it three times. We all know that the email messages were attached, and so this example is a no-brainer. I don't take anything away from your point. Your point is correct, right? If someone submitted in text the headers only, it is possible that they could have altered the headers, right? That being said, they provided some evidence. Maybe that's a more difficult case. Here, it's a no-brainer.

And so, as an example, I think this is a perfect example of an email or a situation where you just decide and you don't waste a lot of time. I mean, if you're a registry or a registrar, why do you want to waste time on this one? This one is clear. Other ones require more information to protect your customers or other people. This is not one.

JEFF BEDSER If the headers are predetermined.

SARAH WYLD We're going to hear really quickly from Luc and then Volker and then move on.

LUC SEUFER Just to say it's a no brainer if the headers are confirming it. Because sometimes has to be a photo in, we look at it. And when you look at the headers, it was not sent through the domain name or the email service attached to the domain name. So once the header is one thing, you have them, but you need to review them. It's not no brainer, you need to check, but yeah.

MARC TRACHTENBERG No, I agree with that. You should check the headers and email. In this example, the messages were included, assuming that they confirmed that it was sent from that domain name. Then, yes, I 100% agree.

SARAH WYLD All right. Volker and Michele, I will give you a moment also, but Volker had his hand up first.

VOLKER GREIMANN Yes, I absolutely agree. This is one of the easier examples where, therefore, the lean towards decide, but there's always the need to look. I mean, coming from a law firm already provides certain

assurances that what they are saying is more likely to be correct than if it came from John Nismo. We don't know who he is. We will still need to check some things when we receive that. There is no such thing as an automatic shutdown. But ultimately, the quality of this report and the evidence attached is a very strong lean towards that.

We also receive similar complaints where any evidence is lacking. They're just saying here's a phishing email that we received. They're not even telling us which domain name is the problem. And that's being sent to three different registrars, because one is in the from field, one is in the link in the mail body, one is in whatever. And are you really expecting us to filter through five different domain names that are in our systems, whether they even register with us? Tell us what the problem is. So, in this case, this is not a problem. So just making that point.

SARAH WYLD Thank you, Volker. Michele, last word.

MICHELE NEYLON Yeah, sure. Marc, I think the problem here is that what you don't seem to appreciate, and I think you're doing this intentionally to a degree, just slightly inflammatory. We have to verify. Pretty much all of us, I think, would suspend or take some kind of action. But it doesn't matter whether somebody has sent us the emails or not. We're still going to have to look and see and check. Look at what's

in the account. Look at the domain age. Now, all of those things. We're not talking about taking days or weeks or that the result of this is inaction. But you can't keep saying, oh, this is simple. Oh, this is it. We still have to check things.

Because one of the things that a lot of us will do is we'll find out that, okay, that domain's dodgy. There are other domains in there that potentially are problematic. Oh, wait a second. How did they pay for that? Oh, great. Now I've got a credit card chargeback coming. I've got a bunch of things. You're looking at IP addresses where they logged in. You're looking at the IP addresses where they signed up. It's not simply a case of I'm just going to throw the switch on this one thing and fix that for you.

MARC TRACHTENBERG To be clear, I'm not suggesting that you don't look at any of those things. I'm not saying that you just get the email from John and you take it down. I'm saying once you look at the email message quickly, you verify the header, say that it came from that domain name, and maybe you look at some of the other things, too. This is a no-brainer. So, again, clarifying, not saying just automatic, not saying just take it down, but saying this one is one where you look at it quickly, and in about a minute, it's pretty clear of what it is, and you can just move on to the next one.

SARAH WYLD: Thank you, everyone. Thank you, Marc. We are going to move on to the next one. All right, last word, Jonathan.

JONATHAN ZUCK: Some of it's just coming down to our definition of decide. That's really the issue. I think looking at the evidence that's provided is implicit in a decide vote. It's not like, oh, I got an email and I'm going to decide that. I don't think-- Except in the case, like I said, if it's a trusted notifier or something like that, maybe. But I think actually looking at the evidence that came is implicit. I think for those of us on the panel, implicit in a decide.

SARAH WYLD: Thank you. I think you're right. It was difficult to try to summarize the possible outcomes into a series of flashcards and decide without looking might be more applicable. If we can look at it and see, it's clearly not DNS abuse. So, moving on to number three. Oh yeah, I like this one a lot because I get a lot of fake Canada post emails. So, we're going to hear a Swiss Post Report.

REG LEVY: Number three, Swiss Post Report. There is a screenshot. But there is no URL bar in the screenshot.

SARAH WYLD

Sorry, Reg. The next slide might be the email. We had them slide backwards.

REG LEVY

It's backwards. Okay, cool. I'm not going to read all that punctuation. I considered it. Report type is phishing. The phishing is ongoing. There is a date and timestamp. Threat Actor is choesz.live, with same source URL. The TLD is in .live. There is a screenshot that we will see in the prior report. And the target is the Swiss Post. The reporter is lruopencti, and their organization is URL Abuse.

SARAH WYLD

Thank you, Reg. And if we return to the previous slide, thank you, Zoe, we have helpfully included Google Translate results for what this page said. So, it includes the parcel number. It's pretending or claiming to be a delivery error notification, a parcel has been returned, and it does have a call to action with a please update your address and a next button. So, it's not a login button, it's a next screen button. And as noted on the screen, it did not include an actual URL bar to indicate that the screenshot really came from the reported domain.

So, our Zoom poll is happening. Our panelists are considering their choices. Does anybody have questions or thoughts as we work through this? Okay, I'm going to be a little bit more organized this time. So, we're going to, in a moment, close the Zoom poll, then

ask our panelists to say what they said or show what they said. How are we feeling? We're there, we're happy. Zoom poll slowed down. Zoom poll has not slowed down. You guys are doing great. We're getting so much. I appreciate all of your input. Yeah. Okay, five more seconds.

All right, so we will close our poll. Thank you. And panelists, what do we think should happen here? Ooh, a bunch of looks. That's exciting. All right. Now, has anybody not had a chance to speak? I think we've all-- Maybe Jonathan hasn't had a chance to go first yet. Would you like to go first? Oh, sorry.

JONATHAN ZUCK I sound much more wise and sage when I've had a chance to listen to everybody else speak and then crystallize the issue at hand. But I said look because it felt like something that required additional validation by the registrar to understand that there was some missing information and it would require some double checking.

SARAH WYLD Yeah. I don't know what web domain the Swiss Post operates under. Maybe that really is it. Jeff, you wanted to speak?

JEFF BEDSER Sure. Thank you, Sarah. So, this is an example that I provided, and I thought it was a great example. It demonstrates a certain problem we all see that we deal with abuse reports is that many times

reporters have screenshots that they've provided prior, and they use it as the evidence. This time as well. Because they're trying to basically demonstrate repeatedly. And because the URL itself does not match Swiss Post and there's no URL bar on the screen capture, there's no way to verifying that this came from that. And in our process, we actually go for a second screenshot to compare, and we were unable to find one.

So, it very well may be that this domain was used for this, but there's no evidence of it that can be used, which is why it's a look. You have to go find out can you prove to us that the screenshot came from that? And that's the look. And go back, and maybe even ask, do you have a screenshot with the URL bar captured so we can demonstrate this?

SARAH WYLD Thank you so much, Jeff. Volker, I see you wanted to speak to your selection.

VOLKER GREIMANN Yes, it was also a look with a very heavy lean towards ask in this case. The evidence is inconclusive. We would try to reproduce the screenshot by looking at the website. If we can get the same result or a similar image if we access that site from various sources, then we would take that as sufficient evidence, the confirmation of the screenshot. If we cannot replicate, we would reach out to the complainant and tell them that, look, the evidence you provided us

is inclusive. We will be closing this ticket for now. If you feel this was incorrect, please provide a correct evidence with URL bar.

SARAH WYLD Thank you, Volker. Mason.

MASON COLE Thanks, Sarah. Volker actually just said a lot of what I probably would have, which is all on target. If I could raise ask and look at the same time, I probably would in this instance, because I'm no technologist, but it looks like this is an incomplete report, and there's an opportunity to learn more about what's going on.

SARAH WYLD Yes. And so, I think it's a good insight that we don't actually have to be limited to one response. This is a limit of the Zoom poll technology and the little panels I made. But in reality, maybe multiple things do need to happen at the same time, or closely thereafter. Let's see the results of-- Wait, sorry. Do any other panelists want to say anything here? We'll come to you in just one second. Zoom poll results up. And please go ahead, sir.

PAULO MILLIET ROQUE I'm Paulo Roque from the Brazilian Software Association. This kind of emails and messages came mainly in Brazil through SMS. Most package customs charge something to clear customs, and they send this fake message asking for, let's say, 20 reais, what be $3, $4,

$5. And maybe people are going to pay. And then they are trapped. What we're doing now is set up a team for DNS abuse and asking all our associates to send this message to us for us to treat them. It's very common just in Brazil. It's getting bigger and bigger and bigger recently. Thank you.

SARAH WYLD: Thank you for that. Yes. And I appreciate the reminder that it's not only email and websites that deliver this kind of problem, but also SMS, right? I often don't think of SMS because it's not a domain name, but it can be used for abuse. Our Zoom poll shows that most people selected to ask for more information. We had a pretty good second, even split between deciding and looking for more info, little bit of outreach, and this time nobody said to ignore it, which is great. Would any other attendees like to speak to this and what they think should happen here. Yes, please.

VIVEK GOYAL: Hi, this is Vivek Goyal. Quick question. Sometimes these websites, they turn themselves on and off. So, it's quite possible then when the screenshot was taken, and even if they give a timestamp, it was there. The moment when somebody from your team was looking at it, it's not there. Would you recommend the requester to provide what so that you would be satisfied to say, yes, this guy keeps turning it on and off so we would take an action? Thank you.

SARAH WYLD

Yes. Thank you for pointing that out. Sometimes it's turned on only for a brief time, on and off. Sometimes they're geo locked in a certain way. So, if you set your geographic location to be in a certain place, then you see the abusive site. And if you're not there, you don't see it. Very difficult to respond to. And I think this speaks to why the report needs, to in the screenshot, include the URL bar because it needs to show that it really was on that page. And even still, I guess people can make all kinds of images these days. Volker, you wanted to speak to that, and then we'll go to Michele after. Thank you.

VOLKER GREIMANN

Yes, with the geo-blocking, that's a very common practice amongst criminals, because they, of course, realize that if we cannot replicate, then it may take longer for a takedown. Therefore, it's advisable for reporters to, if they have that information, tell us, look, this can only be accessed from a Brazilian IP if you use a Brazilian mobile phone network to access this. Or it has to come from a mobile device, for example. Otherwise, you won't see that. If they tell us that, we can take that into consideration and not just go there, see there is nothing there and say, oh, nothing we can really do. The more information we have about how this scam works, the better we can react to that.

VIVEK GOYAL

What about the on and off of the website?

VOLKER GREIMANN Same. If you, as a reporter, have seen that, that's something that you should include in the report. We also try to look at archive sites. We look at sites that have screenshots of such pages before. Some URLs scam detectors or scanning sites and have historic screenshots and if somebody looked them up when it was online, we can see that. So, there's ways around these kinds of circumvention methods as well. But we need to know that this is being applied and then we can work with that.

SARAH WYLD Thank you, Volker. Michele?

MICHELE NEYLON Yeah. This is Michele again. This kind of scam, we see a huge amount of them coming via SMS in the Irish market. What is deeply disturbing is that some of the scumbags have worked out how to insert their fraudulent messages into the iMessage threads. So, you've got legitimate message, legitimate message, legitimate message, scam, scam, scam, legitimate message. And the issue here is often it does involve domains, often it doesn't, but the problem is something that the telcos need to work on. And in some markets, they have taken action, in others, they have sat on their hands and pretended that they can't do anything. Which is untrue.

And it's very much a case of not all of the ills of the internet can be fixed here. You need to be talking to communications regulators

and others. Because like SMS, bulk SMS, I used to be able to send text messages from each and every one of you if I had your number. It would arrive on your phone from me. And there was no validation. Nothing.

SARAH WYLD Wow, thank you. All right, have we any further thoughts on this Swiss Post example? Maybe one day my Canada Post parcel will really get to me. They're on strike right now, I'm told. Again. Okay, we shall move on to number four. Reg, please. Thank you.

REG LEVY Number four, Fake Shoe Shop report. I paid for an item on this site and have not received it. I have been deceived into giving them my personal and financial information, and since then my credit card has been having fraudulent transactions on it. DNS pivots data. The domain is five days old, and there are three other domains hosted on the same IP using the same site template with clothing products and the other with gardening products. The domain names are also of the same structure, (letter)andshopper.tld, and are less than 10 days old. Sorry, but they are in fact fewer than 10 days old.

SARAH WYLD Thank you, Reg. We took these reports exactly as they were provided. I also did not add a comma. Let's look at the screenshot. Yeah, those shoes, right? I want that boot that's right there in the

middle of the page, but I know if I buy it, Canada Post is not going to send it to me. Okay, so our Zoom poll is up. I see people are thinking about it. I see our panelists are thinking. Does anyone have questions? Does anybody have ideas? Yes, let's go back to the report page. Absolutely.

Okay. All right, the Zoom poll is still happening. So, we're going to give people a couple more minutes. I myself try not to buy shoes online because they just never fit, right? All right. They're still coming in, so we're going to just give almost five more seconds. Okay, all right. We shall close the Zoom poll. And, panelists, what should happen here? I see ask, I see look, and I see another ask. Very good. All right. I'm just happy that we're not all saying the same thing because it's more interesting. Volker's got his hand up, so we'll go to Volker first.

VOLKER GREIMANN

So, this is an interesting one because the first part is partially irrelevant. The second part basically provides me with the information that I actually can take an action on, potentially. It's not DNS abuse, necessarily. We have no evidence of that. While they're claiming that their credit card has been stolen from that site, that could be correlation, not causation. There's no evidence of being deceived. There is what could ultimately be a commercial dispute between two parties, where someone has just not received their parcel. That's something that I cannot evaluate. That alone would probably be a rejection of the complaint for lack of evidence.

However, the domain name being five days old, similar domain names being hosted at that IP, the time plate being the same as known fake shops would allow me as a registrar who has a policy against fake shops, not because of DNS abuse, to take action on that basis. Most registrars would not be required to do that under ICANN policy because fake shops are not covered by that. They're not necessarily phishing, but we choose to take action on that. And I've spent many a morning just to go through the registrations of certain resellers to just brand them, brand them, brand them, brand them, brand them, brand them, brand them, brand them, just able.

SARAH WYLD Thank you, Volker. Owen, I know you're having Zoom problems. Here you go.

OWEN SMIGELSKI Yes. Thanks, Sarah. So, I think, Volker, sort of I agree, but I also disagree a little bit as well, too. Yes, it's a five-day-old domain name, so they paid for it. They haven't received it. I don't know where they live, if they expect it to get same-day delivery or how that works. But just broadly, I know that there are terms thrown around about fake shops. I think those terms need to be explored a little bit more. Because there is one type of a fake shop where it may be selling unauthorized from the trademark owner goods. They may be knockoffs, they may be legitimate, they may be gray market goods counterfeit, I don't really care, but as long as

somebody's paying for and receiving something, then that's more of an IP dispute as opposed to somebody's being scammed.

I see this as different where this is a shop where you're paying for something, you're not getting anything, they're stealing your money, they're using your credit card elsewhere. I think that's something a lot more stronger to action and is an example. Perhaps it's not meeting the definition of phishing or whatever, but it's theft. And that's something that I would not want one of my customers doing. I lean more towards suspending. Thanks.

SARAH WYLD Thank you, Owen. We have a good queue here. So, we'll go to Theo next, then Jeff, then Michele.

THEO GEURTS Yeah, thanks. So, this is a bit of a tricky one when you look at a timeline. I mean, okay, I know everybody who orders something online wants it the next day or the next hour. But five days old, and sometimes there's supply chain issues. So, that could be an indication that the product may still be being sent off to the customer. So, you've got to take a look at a little bit of the timelines. In general, when you look at this, you really got to look at the registrant info, look at the website itself. Does it comply with the EU e-commerce directive?

So, you're going to look a little bit of does the location, the contact us website-- There's usually a contact us. Does that match with the

registrant info? So, you got to really do a real deep dive on this. I don't like these ones because they consume a lot of time, especially if you have a lot of them, unless you can confirm that the template is indeed being used. But then I go like I need to see at least 200 of them that have a similar template, not just two. So, you really need to build evidence here to make a decision. Thanks.

SARAH WYLD Thank you, Theo. Jeff?

JEFF BEDSER So, this is a great example of fraud by deception being alleged. And you've got fake shops, which is a fake shop versus a shop that sells fakes. And this is alleging to be a fake shop, which is a fraud by deception, which is basically the same exact infraction as phishing. It's fraud by deception. But I agree to the points that the other panelists, and Theo has made that. There's really suspect when, yeah, the domain's five days old, that's a big red flag, but also someone claiming that they haven't received their product yet, and there's all types of transactions on their credit cards already. That's a look, it's an ask. You've got to demonstrate that.

Because, as Volker made the point, someone who falls for one fake shop doesn't mean that the transactions on their card aren't based on them falling for three other fake shops in the last two days. So, that correlation does not imply causation. So, this is a look. Based on me being three to five days old, and there's three selling

different products that have all launched at the same time, definitely worth looking into but need some more evidence.

SARAH WYLD

Thank you, Jeff. And Michele, just one second. We're first going to see what the-- we're going to put up the results of the Zoom poll. They're coming. And while we're working on that, we will have Michele share his insights.

MICHELLE NEYLON

Yeah, thanks. Michele here. I think there's a few things here. We tend to look at young domains as being of higher risk, but in most parts of the world, five days for a delivery is not that strange. I can't even get a delivery from a brewery 100 kilometers away from where I live in two weeks because the courier is messed up again. So, I think that we send it to me. I've been dealing with them by email the last couple of days.

So, I think the thing here is that this case is one of those ones where I'll be like, okay. It's possible that something hinky has happened, that there is fraud. But we need to know a lot more. Just because you're saying that you didn't get the thing, just because you're saying that there's dodgy transactions on your card. I would probably be asking them, I'd be saying, okay, if this really happened, have you reported this to the bank, have you reported this to the police? And let's have a look at other things. I'd be very, very wary about taking an emotive thing, because God only knows

when we get this kind of thing where it's like, oh, Customer X provides a crappy service. I'm like, yeah, that happens. Is that fraud? No. They're just a rubbish shop. But it somewhere else.

SARAH WYLD Thank you, Michele. Paulo.

PAULO MILLIET ROQUE What impresses me is how a site with only five days old can reach so many customers. They spend a lot on Google AdWords. How do they do that? It's too young to reach so many people. Thank you.

SARAH WYLD Somebody finally paid for that list of shoppers that they're always spamming me to buy. Our poll results are up, and I see there some people have selected to outreach and some have selected to ignore. And we haven't really heard from those perspectives here. Would anybody care to speak to those selections? Okay. Any further thoughts? Any panelists who haven't had a chance to speak to this one and want to say something? Anybody going shoe shopping after this? Are we inspired?

JONATHAN ZUCK I think Michele should move closer to civilization, but that's just an umbrella point.

SARAH WYLD: Maybe the fault is in the brewery. They have to brew it first. Okay. Yes, please come up to the mic.

BERTRAND DE LA CHAPELLE: Bertrand de La Chapelle for the record. What I find interesting in both this case, fake shops, and the previous one regarding the post thing, is that it's everything that has been said shows how difficult it is to take one case and evaluate it. One of the challenges is how to detect the patterns that are emerging, like for the post thing. There might be a pattern in the type of URL that is being used, there might be a pattern in the type of format that is being used. And likewise, here, it is likely to be a coordinated action that there will be several fake shops of the same sort that will be there just for a short period of time. One of the key challenges that we have in addressing abuses is how do we gather the information so that those patterns can be detected.

SARAH WYLD: Thank you, yes. And so, one of the things I liked about this example that we didn't have in the others, which is also fine, is that this one spoke to some of that pattern. And that there's other domains with the same site template. Maybe not determinative, but maybe useful as part of the consideration. Any further thoughts? I see an old hand, I think. All right, let's go to number five.

REG LEVY

Number five, Fake Baby Oil Shop. Report: The website linked to oilbabyoil.tld, is a fake shop. It is used to sell oil baby oil products which are trademarked products by our client, Mr. Sean Puff. This is therefore a phishing website, and as an ICANN accredited registrar, you must take action under RAA 3.18. You must suspend this domain name.

SARAH WYLD

Thank you, Reg. And there was no screenshot provided to accompany this example, I believe. I don't have my slides up in the other window. So, we will open our Zoom poll to see what people think should happen in this case, as I go back to it and confirm that there is no such screenshot. And that's okay, right? The point of this is sometimes that's all you get. Yeah, sometimes that's all you get is just someone saying this is an important thing that is happening. And we're lucky here that they included what the domain name is, because that's not always a given. I see that our Zoom poll is happening. Michele, did you want to speak right this second? Go for it, yeah.

MICHELLE NEYLON

Yeah, thanks, Sarah. It's Michele for the record. I suppose one of the things here is that we have terms of service as well. To be perfectly honest, a lot of these issues that are being discussed here, we'd be looking at them in terms of, well, terms of service and just general legality. I really don't care what's in the bloody RAA. I care

about the fact that a client of ours is doing something scummy and that's in breach of our terms of service. End of.

So, for something like this, I might happen to take an issue with it and look at it in a particular way. But for some of a lot of the other ones, if you found evidence of something, you take action because that's the right thing to do and it's breaching your terms. It's not because you're looking at whatever article in an RAA, be that the ICANN one or a contract you might have with the ccTLD or something else.

SARAH WYLD Thank you, Michele. All right. So, our Zoom poll has slowed down. We're going to close the poll. Does anyone--? Yeah, there we go. All right. And panelists, what should happen here? All right. I see some decide, look and ask, all right. Would anybody who hasn't spoken in the last example want to speak? Rida, please go ahead.

RIDA TAHIR Thank you. I'm Rida. I'm here from the GAC. Sorry, I just out-brewed Reg. I have a very simple rationale. I just don't think the report is very informative? Is that normally how reports look like?

SARAH WYLD Thank you, Rita. This is often how reports look. One thing that we might consider doing is looking to see is this actually a trademarked term, and who owns that trademark? And that might

be something that's included in a report. Here it is not, but it might be something to include in one's investigation. We could ask about it, yes. Thank you. Anything to add to that? Great. Michaela, please.

MICHAELA SHAPIRO: Yes, hi. Michaela for the record. I think one thing I just want to encourage us to bear in mind is not everyone who files these kinds of reports is perhaps an expert in how to make a very useful report. I can speak as myself. If I were to be someone reporting, I would need a little bit of training to understand what kind of evidence you really need to take action on this. So, I just want to bear that in mind. So, that's why I would take a look. This might be a very legitimate claim. This might be someone English isn't their first language. I just want to bear that in mind. But it also could be absolute nonsense. And so that would probably be quite clear from a quick look. So, I would just encourage us to take a look.

SARAH WYLD: Thank you, Michaela. Yes, Jeff?

JEFF BEDSER: This, to me, is a great example of verify the report, don't trust the reporter. In every single case, it's about verifying the report itself to see is it actionable or not. And there's really, this is an ask, this is a review, it's a look, because there's not enough information to take any action based on what they provided. There's no evidence.

So, while what they're alleging is serious enough to get a look, but give us the evidence that we can do something with it.

And to the point of, yeah, an inexperienced reporter. Nice thing about the change in the recent agreements that you can use forms as well as email is forms can require an evidentiary standard of submitted data so you have something to work from, whereas an email-- I mean, we've probably all seen the ones where it's a rambling email of 17 pages of text. And somewhere in there, Grandma got catfished is what they're trying to tell you. But it takes 10 minutes to figure out what they're trying to tell you the harm is. So clear, concise reporting really benefits those that can take actions.

SARAH WYLD Thank you for that, Jeff. Now, before we move to hearing from our attendees and seeing the poll results, before that, do any of our-- I want to hear from the deciders. I saw some blue signs over there. And yeah, thank you, John.

JEFF BEDSER This one was also pretty easy for me, because it's not. It's more of a trademark infringement case. As Michele said, you'd go after it with a terms of use or a trademark infringement lawsuit. It's just not fitting the definition of phishing. So, that was the issue I had with it.

SARAH WYLD Yeah, thank you. Not every bad thing on the internet is DNS abuse. Volker, last word from the panel at this moment.

VOLKER GREIMANN Yeah, same here. It's decide because they're not telling you whether the baby oil is made of real babies or-- The trademark dispute is really not something that we would decide. Could be grey imports. We don't know anything about how they market their product. It's simply something that we would say this is a commercial dispute that you will have with the other party, resolve that through regular courts. And while we've been speaking, I've been taking down fake shops. Currently, number 100 is going down. Thank you very much.

SARAH WYLD So efficient. Okay. So, do our Zoom results show? We got a little bit of outreach, a lot of asking for more information. That might be relating to asking for, do you actually own a trademark for this term? We've got a couple deciding, a couple looking, ooh, and more ignoring than I expected. Would anybody like to speak to why they would ignore this report? We just don't care about what Mr. Sean Puff thinks. Is that Puff Daddy? Is that the same person? Okay. Yeah. I don't know what he has to do with baby-- I guess I'm going to look something up and learn something tonight. Thanks

everyone. You'll tell me later. Okay. There's maybe more implied here than I realized. We'll go to Reg next.

REG LEVY

Reg Levy from Tucows. Despite my mellifluous enactment of this, this is basically incomprehensible to me. So it may, in fact, be a joke, a hilarious joke. I understand that they probably obfuscated the domain name, but oilbabyoil.tld doesn't do anything for me, and so I might just file this in the circular bin. And if ICANN sends me a compliance notice because I never responded to this, I would legitimately say, I did not think this was a legitimate report because I could not make heads or tails of it. I don't see where trademark products happen. I don't see where phishing comes into it. It's just not comprehensible.

SARAH WYLD

Yeah, thank you. I do think that in the real report that would have been provided to the registrar, it would actually show the real TLD and not just say .TLD. It's been obfuscated for here, but sure. Reminder that if you're speaking on this mic, it doesn't lower your Zoom hands, so you might need to lower your Zoom hands. And we'll come to Chris next, please.

CHRIS LEWIS-EVANS

Yeah, thanks. Chris Lewis-Evans for the record. I would ask, but it would be required, I think, to give them some more information about what you're looking for. And I see Ashley's put a reference

for reporters in the chat, so I think just giving them that information helps educate them. I think there is a couple of people said they might not know what to do. This might be real, it might be a proper phish, and that's just a really rubbish report. But you can't do anything, to Reg's point, you can't do anything with this. So, give them some information. How do you report properly? And wait and see if they come back. Otherwise, it would be do nothing. Thanks.

SARAH WYLD Thank you, Chris. Michele, please.

MICHELE NEYLON Yeah, thanks. Michele for the record. I'm concerned about the people ignoring us. Because really you shouldn't be ignoring the report. When you say ignore, you mean you're not going to take any action. Okay, fine. But ignoring the report completely is not the correct way of dealing with us. Most reporters deserve a response, even if the response is, I'm sorry, I don't understand what you're asking me to do. We get a lot of those. We get some stuff through involving trademarks. We had one person who reported a trademark infringement to us multiple times, but wouldn't tell us what the trademark was, and wouldn't tell us how the trademark was being infringed. I'm not a trademark lawyer, but Holy Mother of God, what do you expect me to do with that?

My understanding, and I think it's just generally within an industry, it would be that when you get an abuse report, you should respond. There are one or two reporters who unfortunately have their system set up, and the reports they send you literally say we are sending this from a mailbox that cannot take responses And I wish they wouldn't do that.

And I think Michaela's point about not knowing what we need is really, really important. Just flippantly saying this report is crap, I'm not going to do anything isn't particularly helpful. Asking her, can you provide more information? Can you explain this a bit better to me? Because I think as Jeff says, we've all got these ones where they spend 25 pages telling you about the number of trademarks the Bank of America has and include them. I don't know why I need to have the damn things included. And then you're looking, trying to work out what the hell the problem is. But I think there's a lot of things that are ignoring is not good.

SARAH WYLD Thank you, Michele. Beth. Beth, where are you? Yeah, please.

BETH MARTY Hello. Beth Marty with Name.com. So, I think this is interesting because it actually conflates some pretty core and foundational concepts. It says that it's a fake shop. It's used to sell products. So, that sounds like it actually has sold products. Somebody has actually received something. But then it makes a conclusion,

saying it's therefore a phishing website. And then they say, you must suspend this domain. So, it sounds more like someone who might be familiar with trying to get something done.

And this is pretty classic in terms of when you're faced with in this type of information, why must you act? Which bucket is this in? I wouldn't want to ignore it, but I would want more information. Because if it's fraud, if you're receiving a product that's not actually the real product, that's one thing. If it's phishing, you're never going to receive a product. If it's a trademark dispute, that's entirely another. And if you say they say, you must suspend this domain, that person is after something. And so, I think I'm in the camp of we need more information.

SARAH WYLD Thank you, Beth. Yeah, honestly, the first thing I thought when I read this was, don't tell me what to do. Vivek.

VIVEK GOYAL Thank you. I'm so glad to have Michael said that don't ignore and please respond. In my list of all the complaints we do on behalf of clients, the biggest chunk is where we never heard back anything after we filed a complaint. So, thank you for saying that. It would really helpful because when clients come back to you and say, give me an answer, give me an answer, we can say it was refused. Sometimes it happens we have told them it was refused and after two months the action was taken. And now the client is saying, I'm

not going to pay for this because you said it was refused and now it is down, so you didn't do anything right? So, thank you for that.

I think while you all as a Contracted Party House receive a lot of complaints like this, we as ones who are talking to brands receive so much request from our clients who actually pay us to do this, saying take this down, take this down, this is DNS abuse. And so much time goes in educating the customer that this cannot be resolved through this. You need to find some other way to resolve. Just because I am helping you with something on internet, it does not mean I can resolve all your trademark complaints and your competitors. So, I understand your pain. And trust me, I would like to be a trusted notifier with somebody so that I can learn from you and it will help me do my job better and maybe send less crap towards you to take down. So, thank you for that.

SARAH WYLD

Thank you for that, yeah. And I think the education piece is really important. So, one of the things that the Registrar Stakeholder Group has offered is-- maybe it's from the Contracted Party House, actually. I've lost track. But it's in the Zoom chat. Ashley shared references for reporters, what we need, and it's a PDF link for how to make effective DNS abuse reports. This one might not be DNS abuse, but if you do have some, that's how you report it. Okay. We have time for one more example because we've got to wrap up at quarter past. So, let's see number six. Oh, yeah, I like this one.

REG LEVY

Number six, COVID-19 Pandemic. The reporter is not the domain owner. The offending email addresses are coronavirus.status.space and CDC-Covid19@cdc.gov. The offending domain names are coronavirus.status.space, coronavirus-map.com, blogcoronacl.canalcero.digital, so actually that domain is canalcero.digital, coronavirus.zone, coronavirus-realtime.com, coronavirus.app, coronavirusaware.xyz, although that is not the domain provided. They say bgvfr.coronavirusaware.xyz, coronavirusaware.xyz.

The email header says COVID-19 Everything you need to know, and Coronavirus Update: China Operations. The report is: A report from cybersecurity company Recorded Future noted a significant increase in website registrations related to the CoVId-19 virus, some of which it believes are being used to either pilfer information from recipients or infect them with malware.

There are, for instance, domains registered that appear to come from the United States Centers for Disease Control and Prevention, CDC, when, in fact, they're from dangerous spammers. Researchers have already found one malware that was spread via the legitimate looking email address. Cybersecurity company FireEye provided Forbes, which is a link, with a handful of example spam emails which are attached.

SARAH WYLD

Thank you, Reg. And so, I'm just going to note that although the report says they've included headers, what they've actually provided is the email subject line. So, that's an education issue. Let's look at the next slide, which has a screenshot. My Zoom is no longer happening, but there we go. So, there's a screenshot and it does sure look like that email that they've just talked about. Next slide is another screenshot.

Our Zoom poll is up so our attendees can think about what they think should happen here. Yeah, like, upload it with iCloud Drive. It's not. It's either Google Drive or it's iCloud. iCloud drive is not a thing. What is going on? Let's go back two slides, so we can just look at the example report together. And as we're thinking about it, I see that Zoom is happening. Our panelists are thinking about what their outcome might be, or their next choice. How are our panelists doing? Are we feeling good? We're feeling ready? How's our Zoom poll going? We're still getting a lot of responses. So, I'm going to give the Zoom poll another moment.

Another red flag here, the CDC sending reports. Not going to happen nowadays. Okay. Any questions or thoughts as we continue to finish the Zoom poll? Yeah, I do see some interesting back and forth in the Zoom chat as to whether this report is helpful or not helpful. We're going to give it another five seconds on the Zoom. I see a hand from an attendee. We are going to hear from panelists first, but I appreciate your enthusiasm. Everybody, you're all being so interactive. This is great. So much fun. Okay, we'll close the poll. Thank you for that. And panelists, what do we do?

Ask, ask, ask, look, look, ask, and look. Excellent. Okay. So first up, let's hear from Michaela. I saw your hand really briefly. And we'll go to Volker after.

MICHAELA SHAPIRO: Yes, thank you. And I agree that this report is maybe not the most useful for registrar, but I would want us to take this seriously, given the potential real-life ramifications of not taking action on this. So, I would want to get more information, do the research to flesh out this report. I think there's not enough to know exactly what to do right away, but at the same time, there's an urgency here to take action, given the real-life implications of what this could mean. Yeah, I'll stop there. Thanks.

SARAH WYLD: Thank you. Volker?

VOLKER GREIMANN: Yes, this is an interesting one and can be used to highlight various things. First of whom is, who is this report being sent to? Because we are getting some reports like that that are just sent to us, and some of them are sent to every registrar and registry in the world. The latter ones don't allow us to identify in an easy way without checking which of these domain names are registered with us. So, what we would first do is look at the first name, if it's registered with us, and then the second name.

If neither of them are registered with us, it's immediate feedback to look, we're not going to check a dozen or a hundred domain names that you've sent to us, whether they are registered with us. Come back with a concrete example that you want us to check. We're not going to check all the examples. If they are with us, then most likely we will check whether there's harm in those sites. Unfortunately, as you can see with the current US government, lying is not illegal. Misinformation is not illegal. Therefore, that is usually not a basis for a takedown unless we have that in our policies.

I remember that we did have some policies with regards to COVID prevention that did cover this. However, that may not be the case for every single misinformation that exists. So, we would probably reach out to the complainant and ask them to send a concrete example that applies to us. And tell them that unless it violates our terms and conditions, there's nothing we can do.

JEFF BEDSER

So, a little color on this. At the beginning of the pandemic, some of you guys remember that, right? It was recently. A lot of security researchers found themselves at home trying to help, and they decided that they're going to go out and find all these domains registered with COVID terms and just assume they're all bad and started reporting them in bulk. It was done with good intentions, but it was a mess. The majority of them were, I believe, set up to be domainers, thinking they were going to make some money on the sale of this domain for some value with the pandemic.

But of the ones that we looked at, at that time, we only found one that was actionable, and it was not really phishing. If I recall, it was a site that was selling respirators at €3,000 apiece, at a time when hospitals around the world couldn't get their hands on respirators. And it was pretty clear that that's evidence of fraud. But of all the other ones reported to us and there were several thousand. There was nothing actionable on any of those domains. So, that's why I put look here.

Because if they do have evidence of some of these domains, to Volker's point, we're with that registry or registrar and they have evidence of the fraud conducted with screen captures or headers or something, certainly look into it, take them down. But the majority of those domains probably weren't even with the entity that this report was received by.

SARAH WYLD

Thank you for that, Jeff. Would any of our other panelists like to speak to this example before we move on to our attendee input? I want to make sure everyone feels like they've had full opportunity to share. No? Okay, super. So, let's look at our Zoom results, and we'll hear next from Owen and then Michele.

OWEN SMIGELSKI

I thought you're going to go over the Zoom results. A couple of assumptions that I made when I said that I would decide, of course, a little bit of look first, is are these domain names actually with us?

Because that's a very important thing. As Volker said, sometimes people like to send out mass complaints, but if all of them are indeed with us, looking at that evidence there, then that certainly looked like something that I would lean towards taking down.

And there are certain times where you make exceptions to the norm, and for us, that was during the COVID-19 pandemic. We actually started taking sites down due to trademark complaints. If they were alleging that those were 3M masks, or they were not 3M masks or N95 masks, or similar things like that, or they were purported vaccines or purported cures, at the time when there were no vaccines, we were shutting those sites down, even though that was not phishing or something like that. So, the way we approach abuse and what's happening is certainly just based upon the situations and scenarios or what we're seeing. And so, yeah, this is one that I probably would lean to, assuming those examples were correct and those domains were with us. Thanks.

SARAH WYLD Thank you. Yeah, good points. Michele.

MICHELLE NEYLON Yeah, thanks. I think Jeff pointed out something where I think it's really important. During the pandemic, there was this real knee-jerk type thing around some of this space. There was one company that produced a very large list of names that others security companies ingested into their firewalls. And next thing, you realize

that all of the Department of Health in Ireland's websites that they'd set up specifically for COVId-19 were now being blocked. Which was great fun.

SARAH WYLD How so?

MICHELLE NEYLON Because it wasn't even a direct blocking. It was that several of the ISPs were using the security company number 2, but had taken a list from number one, and number one had put all sorts of random crap in there because they were doing really dumb, if it contains COVID-19, it must be fraudulent. And the European Commission put pressure on the .EU Registry to basically block pretty much any domain name containing a particular subset of terms.

So, this one is an interesting one because there's a huge amount of baggage associated with those terms. I think the length of the list of names, if it was with us, the first thing would be, well, are all of these names with us or any of these names with us? I'd be definitely looking for a hell of a lot more information rather than just going, oh my God, this is bad, I have to do something. We definitely have to look a lot more information. I think it's interesting because of the terminology, the baggage that comes with that is really, really interesting.

SARAH WYLD Thank you, Michele. I see that we have Volker and Vivek in the queue and we're going to close the queue there just due to time. So Volker, please go ahead.

VOLKER GREIMANN Yeah, maybe just one more comment here. The fact that they're including a legitimate site, legitimate domain name as offending CDC.gov would already be a very high warning marker that the trustworthiness of this report is probably not that high.

SARAH WYLD Yeah, good point. All right, last word here. Thank you.

VIVEK GOYAL Sure. See, I understand that it's easy to take action when you know the brand name. And if the brand name is in your region, you trust that, yes, it is abused. But there are brand names you've never heard of, which might be huge in the region in which they exist. If that brand name has a dot brand, will it help you believe that it's a genuine thing and will you assess it higher as compared to a brand you've never heard of?

SARAH WYLD That's a question. I don't have an answer to that. Do any of our registrars or panelists want to address that? And it might be

something to think about and take away as a thought for next time. Oh, Michele, please go ahead.

MICHELLE NEYLON: Thanks. Michele for the record. I think it's easier to assess something when you have some knowledge about it. But at the same time, with trademark and IP disputes, my go-to responses often will look pretty much every word in the dictionary is probably trademarked somewhere. And so, you can't just say, oh, there's a trademark there, or you've got a right to do things.

Prime example let's pick on Apple. Apple is a very well-known brand of this, that and the other. There's also an Apple record label. And if I want to sell apples, you can't prevent me from registering a domain name with the term apple in it. But we have had some very aggressive trademark people coming along and going, no, no, no, we have a God-given right to a particular string. And often that string is quite generic. It's not something that's invented. It's not something as specific as Viagra. It's something like virus.

SARAH WYLD: Thank you. We have so much enthusiasm for our panelists. We're going to have Volker and Jeff really quickly because we do need to wrap. Thank you.

VOLKER GREIMANN Yes. To Michele's point, I think trademarks are something that we cannot adjudicate disputes on. That's why the EDRP is there. There are complex legal matters whether the use of a trademark or a trademark term violates a trademark. That's not for us to decide. We also get complaints from reporters that send out AI-generated emails before they think. That, for example, have clients that trademark the term water and then send out emails for every domain name that has the string water in it. So, clearly generic terms. That's the fastest way to get on our block list and never to see any response from us again. And that reporter is on that list.

SARAH WYLD Thanks, Volker. Jeff, last word.

JEFF BEDSER Yeah, certainly. I think directly to the question, Vivek, about brand TLDs, I think that, again, Michele's point about knowledge. Dot Baby, which was a Johnson & Johnson baby products TLD, was then sold and genericized. And there's dozens of others that were bought as trade as brand TLDs that were turned into generic and as a result, you can't trust it necessarily without research who owns that TLD now and how's it being used as the next point.

SARAH WYLD Okay, thank you all so much to our panelists. I really appreciate your insights and participation today. I hope you had a good time. Thank you to our attendees. Before we wrap up, I want to share a

little bit of information about a tool that the Registrar Stakeholder Group offers now. Now we did talk in in the Zoom chat about the resources on our website, which is rrsg.org, and you can find all kinds of explainers there.

But we also have acidtool.com. This is the abuse contact identifier. So, just like not everything is necessarily DNS abuse, not every problem on the internet necessarily has to go to the registrar to solve. But sometimes it's really difficult to find out who is the hosting provider or the email host. So, we hope that this tool will help. And we have just launched a new version. So, you can go to acidtool.com, type in a domain name, and it shows you not only the registrar, but also the hosting provider, the mail host. And right now, it finally does IDNs. Hooray! IDNs are now supported. We've updated the UI. It does an RDAP lookup now, instead of just WHOIS. There is also a backup WHOIS, but it does RDAP, which it needs to be able to do.

There's a click to copy button. It used to be really difficult once you see the results to get them out of the page. Now you just click a button, and it copies it to your-- Yeah. And a few other UI improvements, as well as improvements to the architecture and security. And it works for both G and ccTLDs. It's just everywhere. So, we hope that this is a useful resource, acidtool.com. Also remember, the Registrar Stakeholder Group website, rrsg.org, has a guidance and information section in the header. And if you have thoughts as to what other information registrars can provide, please do let me know. We're always happy to hear it. All right, two

minutes to spare. Thank you very much, everyone. Have a great day.

[END OF TRANSCRIPTION]