ICANN85 Mumbai | CF – GNSO: RrSG - CSI ICANN - DNS Abuse Investigators
Wednesday, March 11, 2026 – 15:00 to 16:00 IST

DEVAN REED

Hello, and welcome to the RrSG: CSI ICANN - DNS Abuse Investigators session. Please note this session is being recorded and is governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct concerning Statements of Interest.

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

SARAH WYLD

Thank you. Hello, everybody. Welcome to our Registrar Stakeholder Group session, CSI ICANN - DNS Abuse Investigators. Thanks for joining us. Okay, next.

It will just be a moment as we switch slides. Okay. So while we're working on the slides, I will do our little introduction. To start with hello, my name is Sarah Wyld. I am the vice chair for Policy of the

Registrar Stakeholder Group, and I do policy and privacy work with Tucows in Toronto, Canada. Okay. So next slide, please, Zoe. And the next one after that.

Welcome to the team, recruits. As part of your onboarding to CSI ICANN, we're going to work through some case files together, looking at the evidence to determine if there's enough there for us to take action. You should all have evidence packets in front of you, and I'm going to post a link in the Zoom chat. There it is. And we have some printouts here in the room. As I just mentioned, if you need one, I think we have a couple more copies with our friend Mohit.

For each one, a CSI agent will take us through the initial DNS abuse scenario, explain the evidence that the team has gathered in each of our five categories. From there, it's up to you. Is it just a series of unfortunate events, or is someone abusing the DNS? Okay. Everybody, make sure that you're in the Zoom Room so you can participate in the polls, and we're going to go ahead and get started with our first case file.

So as we get into this, we will go for each case file. As you see, we have five categories of evidence. We will look at the information that we have for each one, and then vote and discuss, is there sufficient association to suspend the other domains? The first domain in our case file will be confirmed DNS abuse, and we're looking at the other associated domains. You will determine, yes, there is enough evidence. Yes for some but not all of the…

Do I need to grant access to the file? I'm so sorry friends. As I adjust the file settings, we will hear from Reg with our first case file, The Case of the Curious Classifieds.

REG LEVY

A domain was reported to be impersonating a popular online classified ads site. Investigation into several factors led to identification of other domains. Are they related or are we just window shopping? The evidence that you have in front of you indicates that the registration data is publicly available and not obscured by privacy services. All domains share the same registration data, including an e-mail address at a free provider. The domains were all registered within 24 hours of each other. They are in the same TLD, but do not otherwise follow a pattern. The domains were purchased with funds already allocated to the account. The original source was cryptocurrency and the origin could not be further traced. Both domains share identical JARM values indicating that they likely originated from the same server.

SARAH WYLD

Thank you for reading that for us, Reg. I forgot to turn my mic off, but that turned out okay. While we put up the Zoom poll for all to vote, I would like to hear from those of us here in the room or online. Those are the incorrect Zoom questions.

REG LEVY

That's okay, we know what the questions are.

SARAH WYLD: Is there sufficient association to suspend the other domains in this Case of the Curious Classifieds? Do we know if the other ones can be suspended? Any thoughts?

I see a question about what JARM values are. That is a web hosting server sort of fingerprint. In this context, those two were the same, which suggested that the different domains were being used by websites on the same server. Gabriel, please.

GABRIEL ANDREWS: Just to clarify too, when you say that the funds were via cryptocurrency allocated the same account, that means that it's the same customer account that these are all being registered from?

SARAH WYLD: Yes. The same customer account in the registrar had crypto put into it. I see a hand from Owen.

OWEN SMIGELSKI: Thanks, Sarah. It says "other domains". Is this two domains or is this 500 domains?

SARAH WYLD: Thank you. That's a good question. These are real examples that we have just modified lightly to fit into the template. I don't

remember exactly, but I do notice that the very final thing on this page says both domain names. It's possible that there was one abuse domain confirmed and then two more that were identified. With that, do we think that those subsequent domains should be taken offline? Should they be investigated further? Should we just do nothing and move on with our lives? We are still working on the Zoom poll, but we could do a show of hands. Who thinks we should do nothing? I see no hands. Who thinks we should take down both or however many other domains were found? Is there sufficient association to suspend those domains? Yes. Does anyone think just flat out yes? Is anybody not sure? All right. That's useful. Would anybody like to talk about what information they might find useful? I see a hand from Gabriel.

GABRIEL ANDREWS I'm just trying to think about other information that you might have in your possession. I guess you are the registrar in this case, right? You might have, for example, is this both within—you say the same 24-hour period of each other, but are they both registered within the last 24 hours? Is this something that just happened or is there a pattern in practice that these domain's being used for years and years and legitimate purposes? I think that would indicate different potential streams to take, as I think the registrars have often called out, there's a difference between maliciously registered and compromised domains. These are sorts of considerations, I think, raised in my mind and I imagine yours as well.

REG LEVY You are the registrar and this is the information that you have.

SARAH WYLD Thank you. Owen?

OWEN SMIGELSKI I don't recall that it was impersonating a site and then it was suspended. That was all the information that we have on this. I don't know. Was it suspended because of a DMCA complaint, which could be a copyright complaint? I don't know if the reason for was it because it's phishing or something along those lines. That's the kind of information I would need a little bit more to be able to make that determination.

SARAH WYLD Thank you, Owen. It's so helpful to hear what information is lacking that we might need to look for. Graeme, please.

GRAEME BUNTON Thanks, Sarah. It's not clear to me if both domains resolve. Does the second domain resolve and does it resolve to the same thing that the first one did?

SARAH WYLD I'm not sure. Thank you. I think we will move on to our next example. Just a note, there is a bit of an issue with the Zoom polls,

so we're going to do this the fun way without Zoom polls and just hands raised. Welcome to those who are coming in. I think we have a couple more print... We do not have any more printouts, but we will post again the link to the—there we go.

Would somebody like to read the next case? We will have Reg read it.

REG LEVY

The Case of the Identifying IP Address. A registrar reviewing an abuse report noticed an access log for an IP address from a different part of the world than the account information on file. Searching that IP in their system brought up several more accounts it had accessed. Are they all related? Or is it just an IP inference? The domains did not share registration data, but several of them used addresses belonging to co-working spaces. The domains actually used for DNS abuse were registered over a few weeks, and the accounts were in use with other registrations for several months in total. The domains did not follow a specific pattern. They did not use the same payment method. The domains pointed to websites with identical content and used the same provider and MX records.

SARAH WYLD

Thank you, Reg. In this context, we do know about the websites. We will go to the slide for our poll questions. As a reminder the question is, is there enough evidence to take action on the

associated domains? Yes, yes for some, maybe, or no? Does anybody have thoughts as to how they would proceed in this scenario or further questions about it? Michele?

MICHELE NEYLON

Good afternoon. We do see these kinds of scenarios a little bit too often. I think we would probably take action. I mean, the issue for us often is that if the domains have been registered for longer than the grace period, then we're out of pocket. But at the same time, we'll also have to run the high risk of getting credit card charge backs. Basically, I tried to articulate this a bit more clearly. We've had multiple attacks like this over the last year, mostly in ccTLDs. The identifying item that we've been able to track is often a pattern of the e-mail. So it's not an e-mail, it's more that the e-mails follow a kind of a syntax, it's a bit weird. And the addresses are usually kind of very strange.

We would probably take action because that's—an IP address, you'd have to look it up. I mean, the first thing is I'd look up the IP. If the IP is a VPN or something, that changes the conversation. But if it's like a residential DSL, fiber connection, then it's probably a person logging in to that. Where if it's a VPN, it could be anything. It could just be Reg has got an account and he's got an account, you've got an account and you always have to be using the same bloody IP. I mean, that's a totally different scenario.

SARAH WYLD Thank you, Michele. I saw a hand from Gabriel. Super. Graeme.

GRAEME BUNTON Just a clarifying question. Thank you, Sarah. We're talking about suspending the domains associated with the IP address only, not the other domains across these accounts.

SARAH WYLD So in this context, they had the IP address and then they searched that and found more accounts with domains in the accounts. And so they would be taking action on those domains in other accounts that they found by looking at that first IP address.

GRAEME BUNTON It seemed as I first read it, which was quickly, that there are maybe other domains in those accounts that were not registered by the same IP.

SARAH WYLD Hard to say from this example. It's just an interesting feature of putting together this type of thing. We ask very specific questions and then receive answers that don't always tell us everything we want to know. But I think it shows how much investigation really needs to go into this process. Michele?

MICHELE NEYLON

Thanks. I mean, what we've seen happen is that they will sign up using one... For context for those that don't know my company, we're a retail registrar. I sign up from one IP, which might often be an Irish IP because we're an Irish company. Yay. And then once the domains are active and other services are active, then you start seeing logins from IPs in rather odd parts of the world. Let's just go with that. And we would look at what's in the accounts because it might... We've seen some really, really weird ones where we can't really work out what the hell they're doing. We know there's something up about this. And when you have this kind of repeated type thing where you're getting hit with this multiple times, you start to kind of go, "We're going to have to take much broader actions." We would probably suspend quite a bit more than we would do in other instances, because it's the shared IP that's freaking us out a little because that usually means stolen credit cards.

SARAH WYLD

Thank you, Michele. That's interesting. I see a queue building, but I'll just talk for one moment. I noticed something from Gabriel in the chat that's interesting is saying that the key is that they resolve to the same content. What I want to point out is I appreciate Gabriel explaining what factor it is that he would consider as being so important here. As other people think about what their response would be, also think about why and what is the key for your decision.

Then I noticed the question from Bruce in the chat, whether these accounts are new or old and the lifetime of the domains, that's indeed an appropriate avenue to take. What we know here is that they were registered over a few weeks. And my understanding is it's only been a few weeks live and then they found that it's happening and take action. We'll go to Owen next.

OWEN SMIGELSKI: Thanks, Sarah. As Michele was giving his example, I kind of realized why you might find a really weird IP address not associated with—his Irish customer could create up an account. But then he has customers use an offshore, perhaps say Indian-based contractor to create a website. Then they could have the credentials and would log into the website. That might be a very legitimate reason to do so. It will appear really bizarre. But there's a number of reasons why you do that, especially when we're on a global Internet. Don't want to rush to suspend everything just because of a suspicious IP, but also again, if it's bad, take it down.

SARAH WYLD: Absolutely. Maybe one factor is not enough and it is the confluence of many factors that we consider. Andrew, please.

ANDREW CAMPLING: Hi. I guess two things for me. One is on the assumption that you've got effective "know your customer" processes so your confidence is not an account takeover. Then I'd agree with the comment in the

chat, but if it's all pointing to the same content, that to me is the compelling fact on the sheet. But with the caveat that you've got strong know your customer processes, so you can rule out account takeover.

SARAH WYLD Thank you for that, Andrew. All right, do we have any other thoughts as to this one? Michele, thank you.

MICHELE NEYLON I hate agreeing with Andrew, but in this case, I will. I think the thing is that it's the identical content that's a massive red flag. Huge. That suggests that it's all being done by the same actors in some shape or form.

SARAH WYLD Very good. Thank you. Andrew, is that new hand or legacy hand? Before we move on, we're going to do a show of hands in our informal Zoom poll. Is there sufficient association to suspend the other domains? Who thinks no? Who thinks yes? And who thinks maybe but more information is required? Who thinks maybe but for some?

I should have been trying to characterize what the responses were as we were going. I saw no hands for no. I saw a few hands for each of the other options. Thanks, friends.

Let's look at our third example. I'm hearing people training pages. You all make me happy. The third one is our Bewildering Blizzard. Reg, please. Unless somebody else would like to volunteer to read this case file aloud. Francisca.

FRANCISCA CHINWE EZEOBELE Hi, all. The Case of Bewildering Blizzard. It was a snowy few weeks over the Christmas holidays when a registrar and hosting provider saw a sudden and significant rise in registration attempts. Were they valid signups or was it a blizzard of bad domains category? Registration data matches up. Each domain had a new account, unique e-mail address, different set of contact info, and came from a different IP address. Order date and time proximity. Nearly 150 orders were placed in close proximity, each one for a single domain. Domain follows a specific pattern. The domains were random strings of letters and numbers, following no pattern. Same payment method used. The domains were all purchased using the same Payment Service Providers, PSP. Other associations. The other attempts all came from the U.S.

SARAH WYLD All right. Has anybody have thought as to how you would dispose of these domains? Michele? Thank you.

MICHELE NEYLON Thanks, Sarah. I just found it rather amusing the mention of the order attempts all came from the U.S., because that's going to

change depending on where your company is based. If all the orders came from the U.S. and the orders were placed with us, none of the domains were registered, so I don't care, basically, because they won't got through our fraud filters probably. Well, they might have done, but it's less likely. Whereas, obviously, for an American company, it would be quite normal that the orders came from the U.S. I think that's kind of interesting.

The actual domain names themselves, the random strings of letters and numbers, that to me would be probably ringing alarm bells if I've got 150 orders. Now, there's a bit more context to this, I think. Those 150 orders for me are a lot of orders. 150 orders for—I don't know. Who the hell can I pick on?

OWEN SMIGELSKI Pick on me.

MICHELE NEYLON It's far too easy. I keep picking on you, but yes, sure, 150 orders for Namecheap, I doubt they'd even notice us. We would see us. They might not. I don't know. Would you see us? Would you see this? Would you be able to pick up on us?

OWEN SMIGELSKI I don't work on [inaudible].

MICHELE NEYLON: Not helpful. Anyway, I think that's the other thing as well. Depending on the size of the registrar, that's the thing. Because 10 domain registrations for us, sure, normal. 150 random ones all from the U.S. in the space of 24 hours, that's very weird.

SARAH WYLD: Thank you, Michele. The registrar noticed that volume enough to submit this as an example, which I think may tell us something about what their standard volume would be. I see Gabriel next.

GABRIEL ANDREWS: Thanks, Sarah. Again, Michele is bringing up great points. And I think the key thing he's calling out is that context matters. Similarly, if your registrar is in the U.S. and you expect U.S. customers, that means something different than if you are an Indian registrar and you usually have Indian customers, and all of a sudden, you're getting a spike in U.S.-based ones. That would be weird versus normal.

I further want to note that this is kind of a nicer use case and that this is orders and that these domains have not been delegated already. Presumably, your mitigative action isn't going to be take down something that's already existing and potentially harm people, but rather do just a little bit more due diligence if this is raising your hackles.

SARAH WYLD Thank you, Gabriel. Andrew?

ANDREW CAMPLING Hi. I should first say I obviously agree with Michele completely. I mean, the two things for me, the obvious red flag is the random strings is always suspicious, certainly at that volume. And then secondly, the fact they're all using the same payment service provider, it would, to me, be an extraordinary coincidence to have 150 independent customers behaving in the same way. I think this action is required.

SARAH WYLD Thank you for that. I want to note in the chat from Christy in the comment to try to contact some of the registrants to see if there are real and different people behind the orders. That may not be available to every registrar every time, but in this circumstance, that might be useful.

And here's a little secret piece of information that we did not include on the sheet, but you can think about how it might affect your choice. These registrations were not completed because the payment provider flagged them as fraud.

With that, we shall vote. Is there sufficient association? Now, pretending that they were registered because they weren't, but if they were, would they be suspended? Yes? A show of hands. I see so many hands. Anybody say no? I see no hands. Does anybody want to choose a middle option? All right. Thank you, friends.

We shall move to our next case file, The Case of the Bogus Brands. Mohit will read for us.

MOHIT KAMBLI

The Case of Bogus Brands. These days, everyone has their own line of merchandise. A group of threat actors has been registering domains claiming to be the official sites for some very fancy swag. But reports are coming in saying that they take payment and never provide the goods. Are the domains related or is it just hard to find good merch these days? Interesting question.

Some of the domains shared registration data. Initially, these registrants were found to all come from one particular country, but over time they added additional regions. This order occurred over a period of several months, not all at the same time. Domains would often use official dollar brand or the brand's actual domain, but in a different TLD. Payment methods were not always the same. Closer inspection of billing details often resulted in a geolocation mismatch from the registration data, purchaser's IP and billing address. Domains pointed to a few templated websites that looked extremely similar, but not exactly the same. However, they all copied logos from their brand's real websites.

SARAH WYLD

Thank you very much. Just a note where it says official dollar sign brand, that was to indicate that it's a variable. It's the official whatever brand name. I did post the link in the Zoom chat again, if

anybody needs to download their evidence packet. What do we think? Is there a reason to take action against these associated domains? Michele? Thank you.

MICHELE NEYLON: Thanks. I think we'd be looking into it a little, but I mean, my concern a lot of the time is—I'll be honest, I don't really care about the brand. That's not my problem. It really isn't. And we're not customer service for our clients' clients. I'm usually much more concerned around the payment and things like that. Are the payments that we've received going to come back and bite us? That is one of the things I'd be looking at. If this all happened, I think you said it happened over several months, in that case, if we haven't had charge backs by now, we're probably not going to get them. Unless and until I start getting something from law enforcement or anything else, I mean, it's interesting, but I'm probably not going to do much.

SARAH WYLD: Thank you very much, Michele. Who else has thoughts on this one? What are we doing about these brands? Thank you, Owen.

OWEN SMIGELSKI: This might come as a surprise to some people who know me as a trademark attorney. I also don't care about the brands. For me, it's what is the website doing? They're paying money and something's not being delivered, that could be indicative of potential fraud,

where they're just stealing money. That said, how long have they not received their product? Has it been a week? Has it been three months? Because sometimes shipping can be delayed. Have they been tracking numbers and stuff like that? We need a little bit more information on that, but I'm leaning more towards that this is a fraudulent site just because nothing is being received. If they were receiving, say, a knockoff or a fake whatever bag or something, then that's not something necessarily that a registrar can police. Thanks.

SARAH WYLD Thank you, Owen. I see Graeme.

GRAEME BUNTON Thanks, Sarah. I would not personally categorize this as DNS abuse. It feels very much like a fake web shop. And that is to the registrar's discretion. Many I see choose to action such things. Many don't. That is up to them.

SARAH WYLD Thank you. I was hoping someone would say that. Michele?

MICHELE NEYLON Thanks. I put this in the chat, but I suppose some people only listen. I would be a lot more comfortable with a report from law enforcement. Like if you're having an issue where you say that "I paid company X," I don't know that you paid them. I have no way

of knowing this. I don't know what they said. I don't know whether they said that they were going to deliver it in two days and it's been a week or whether it was six months. I have no way of knowing that.

I'll give you a concrete example. If you order a sofa... Have any of you ever ordered a sofa? Okay. What is the lead time on a sofa in Europe? No. But okay, Canadian. It's about 8 to 12 weeks. If you order a sofa and you don't get it next week, that's completely normal. It might be frustrating, but it's normal.

So I would want to report from law enforcement. But then I'm kind of going, "If they've gone to law enforcement, then they are being serious enough about their complaint and law enforcement have taken the complaints seriously." Because we get people coming to us all the bloody time and it drives me bonkers, going, "Website X is illegal." "Okay, go report it to the police. Please, report it to the police. I don't care which police. Report it to the police. That's what they're paid for." Sorry, Gabe, but I mean, it's a statement of fact. It's your bloody job. Report it to them and then they can report it to us and then we can do things. But I don't like this kind of thing. It's illegal. Where? According to what? What's the metric?

SARAH WYLD Thank you, Michele. I think not every bad thing that happens is always DNS abuse. And just for the record, I did order a beautiful sofa. It arrived the day before I left for our Dublin meeting. Sorry,

the day that I left so I had to wait until I got home. It was terrible. Gabriel?

GABRIEL ANDREWS

Again, everything you're saying—is there an echo? Okay. Everything you're saying is reasonable. I'm going to keep talking through it. One thing that occurs to me is that if there's a suspicion that there's crime going on and whoever's complaining to you says they're going to the police and maybe they're trying to prove that to you, even if you don't want to take action on this, one thing that you could do to make our lives easier is if you really think that at some point in the future going to come to you about this, please just don't delete the logs. Preserve. And that would make us very happy in the future. If we do come in with a subpoena search one, whatever it is in the future, if you have the records that are associated with that, that makes life better. Thank you.

SARAH WYLD

Thank you. That's helpful info. Volker, please.

VOLKER GREIMANN

Just to chime in. Volker Greimann from the Registrar Stakeholder Group. Going to the police has also another effect that is very, very valuable for us. Because if you go to the police, the police have a chance to actually catch the bad guys. And if the bad guys are caught and put in prison, they cannot set up a new website the second we take down their old one.

Because the work that we currently do usually feels like we are Sisyphus pushing a boulder up a hill, because anything we do has zero effect. It does nothing to deter abuse. The people that set up these websites, set up these phishing sites, will already by the time that we have a chance to react, made their money back off the registration, they will have already profited largely and immensely. The deterrent of us taking down a domain name is not actually one, the deterrent of being caught by the police is the actual deterrent. Thank you.

SARAH WYLD: Thank you, Volker. Would anybody else like to speak about what they might do in this case? Prasad, thank you.

PRASAD JOSHI: Hi. For the record, I'm Prasad Joshi from Reliance Jio. I just wanted to mention the similar case. As Reliance Jio, I'm a telecom company of India, and not a merchandise, but we provide the recharges for our telecom services. In this case, normally we found domains which are providing the same logos and everything, and they are giving discounts or the sale or the lucky draws where the payment is not there. But they are collecting the mobile number, names, the information of related, not mostly all PII, but part of the PII. In that case, what do you think about it?

SARAH WYLD

It's a good question. Would anybody like to speak to that? I think we'll have to think about that. Thank you very much. Just don't forget to put your hand down when we're done. Thank you very much. We will do our vote. Is there sufficient association to suspend—sorry. I saw a new hand from Michele. Please. Thank you.

MICHELE NEYLON

Just on the gentleman's query there, if I understood it correctly. Again, it's a lot of contexts. I think if you're saying that a website is being used in a particular way, if you're able to show us... Jean-Christophe [inaudible]. If you're able to show us the evidence of what they're doing, if there's something that has better evidence than just simply an allegation, that might be helpful. I think I'd want more, though. I'd want a bit more juice.

SARAH WYLD

Thank you, Michele. All right, show of hands. Is there sufficient association to suspend these domains due to DNS abuse? Does anyone think yes? Do we think no? Maybe something else? We do have some yeses. I forgot to turn around. Thank you. I saw a lot of hands for no, not DNS abuse, maybe a different kind of problem. Do we have any maybes in the room that would like to be a maybe? Always an option. I do not. Okay. All right, thank you.

We shall move to our next case. I don't know what our next case is. The French Phish. Would anybody like to read this one for us? Mohit would like to read again. Thank you.

MOHIT KAMBLI

The Case of French Phish. The registrar was notified of a spam e-mail used as a vehicle to phish; the target, the French health system. They took action, but a few days later, they received a similar complaint about a different domain, but the same phishing campaign. Are they affiliates or is it a false positive?

The registration data was different for each domain. The initial phishing domain was new. The other identified domains were older, registered on different dates and renewed multiple times. The domains did not follow any particular pattern. The initial domain was renewed over several years with the valid payment method used only for that account. Other identified domains each had completely different payment details. The first two domains were initially transferred in from another registrar with about 10 others all through the same account. They were only separated into individual accounts afterwards.

SARAH WYLD

Thank you. Who wants to think about the French health system? Do we think this is DNS abuse? I see hands. Thank you, Michele. I really appreciate your consistent input. Thank you.

MICHELE NEYLON

Thanks. Something involving e-mail, I want evidence, I want headers to start with. The way that these domains were registered obviously for multiple years, that makes me think that they're

unlikely to be dodgy. Scumbags I know are patient, but they're not that patient. I mean, we really need to look at everything we had in terms of data, but I'd probably be saying probably not because it's just the age of the domains that's throwing me.

SARAH WYLD Thank you, Michele. I appreciate that input. And as mentioned, I like a lot hearing about like what is the factor that people really pick up on. We will go to Brandon next. Thank you, Brandon.

BRANDON EASTHAM Brandon from DreamHost for the record. The first instinct on this tells me compromise versus intentional DNS abuse on this one. Obviously, look into it more.

SARAH WYLD Thank you very much, Brandon. Andrew?

ANDREW CAMPLING Hi. I think the age is a red herring, respectfully, because it does go on to say at the bottom about they were all transferred in at the same time by this inferring recently, not 10 years ago or anything. That might be a wrong inference. But on the assumption that's a recent event, I think that's the key piece of information here, which would lead towards potentially taking action, because it does indicate that they are actively involved in phishing, not just there's a suggestion they could be in the future.

SARAH WYLD: Thank you, Andrew. Before we go to Owen, I see a question in the chat from Gabriel. Can a registrar explain more about what it means when the transfer was all through the same account? Would anybody like to speak to that? I see four different hands. I think I'm going to go to Volker.

VOLKER GREIMANN: The way I read that, and it might not be how my other learned friends from the registrar community see that, but the way I read that is that this is one customer that has one customer account in which all these domains were transferred in, as opposed to maybe 10 different customer accounts where each individual domain would have been transferred in, which also is something that we see from time to time.

SARAH WYLD: Thank you, Volker. Owen, please.

OWEN SMIGELSKI: I would interpret that the same way, Volker. I want to agree with Brandon. It seems like the first one, at least for me, that was perhaps a malicious domain because it was a newer "account". But the other one is with the age. That generally tends to indicate that there's something wrong with the site. They packed a WordPress plugin or something along those lines. Usually, bad actors don't

register a domain name, hold on to it for five or seven years, and then start doing something with it. That's just the sunk cost.

There are indications, though, that domains are aged for a degree because as we get different ways to look for DNS abuse, one common factor is registration and then abuse campaign. They'll age it for one, six, several months. Some of them are actually seeing they will wait until the renewal period to do it because then it's almost a year old. That's not necessarily dispositive, but multiple renewals, that, for me, is a sign that there might be something out of account that needs to be fixed. Thanks.

SARAH WYLD Thank you, Owen. Good thoughts. Michele, please.

MICHELE NEYLON Thanks. Ultimately, as the registrar, I'm going to have access to quite a bit more data than what's there. I'll have access to things. I'll obviously have the registration dates. I'll have update data. If I really, really, really wanted to, I might want to have a look at nameservers. There's a bunch of data points that I might want to look at depending on how interested in this I was.

I think the question that we're looking at here is, is it DNS abuse? I would say possibly not. Is it something else? Maybe it is. I don't know. But there's going to be a lot of other data points I have to look at.

SARAH WYLD

Thank you, Michele. All right. We'll do our informal poll. Is there sufficient association to suspend the other domains for DNS abuse? I should have put that in the poll question. Owen has a hand. New hand? Legacy hand?

Yes, there is sufficient evidence. Any thoughts on that one? I see no hands. I see a yes. All right. Do we have any nos? Not enough evidence? I see a hand. I see some hands. Do we have any maybes or need more information? I see several.

MICHELE NEYLON

I took two options.

SARAH WYLD

That's fine. Stuff can be two things. Both is good. All right. Owen wants to speak. Please, do.

OWEN SMIGELSKI

I'd like to vote for a different thing. Not necessarily more information, but if this is a compromised domain, that's less likely of a candidate for immediate suspension and a little bit more to look with the registrant or the host to see, "Hey, fix that WordPress plugin or whatever might be causing that problem." Not to blame WordPress all the time. It could be a website that's got 500 pages and is associated with a university so you don't want to take that down versus if it's a single page used for bad stuff. Thanks.

SARAH WYLD

Very important point. Thank you so much, Owen. All right. Just to note, we have two more scenarios to talk through, two more case files. I'm sorry, but we first have a hand. Please go ahead, Michele.

MICHELE NEYLON

I'm just actually going to throw a little one in there just for a bit of fun. How about actually the TLD itself? The reason I raised this is because not all TLDs are created equally, they don't attract the same users. And I'm looking at this in terms of all TLDs across the entire spectrum, including ccTLDs. Depending on the TLDs involved, that might also be a factor when you're looking at this.

For example, if it was a .bank, it's highly unlikely that the damn thing was registered by a scumbag. Because the .bank TLD makes you have to go off and sacrifice multiple small animals in order to... hand over your first born, baptize a church. All these crazy things in order to get the domain. Some of the ccTLDs have very, very funky requirements. I'm using the word funky, that's a placeholder for other words that I can't use on a microphone or an ICANN meeting. Catch a bit of a beer, I will use it there. And with some of the other gTLDs, again, the likelihood that an Irish company would be registering a domain in Mandarin Chinese probably would trigger a kind of question as to what the hell is going on. There's a lot of those kinds of things I'd look at as well, hypothetically speaking.

SARAH WYLD

Thank you. Lots of good factors. I see a comment in the chat about aged domains. Definitely always makes me think of aged cheese. All right. We will move to our second to last... Yes, everything makes me think of cheese. I know. Second to last sample. And would somebody like to read this one? Please go, Francisca. Thank you.

FRANCISCA CHINWE EZEOBELE

The Case of the Social Scam. A registrar received five separate reports about one domain over a 24-hour period. The domain resolved to an active website that looks like a well-known social media platform, including the brand's login interface, and prompted users to enter their credentials. The user's account held another 180 domains. Are they all social media phishing scams or is it just a suspicious setup?

Categories, evidence. Most of the domain shared the same registration data where it didn't match exactly. There was a partial match. That is the city, street address matched but the name was different. Domains registered entered in clustered batches often within minutes of each other. These high volumes started shortly after account creation. The reported phishing domain incorporated the impersonated brand name. Some other domains in the same account used the same brand name with a word after it. Some used generic commerce terms paired with known trademarks. The domains were all purchased using the same payment service provider under a single shopper account. Heavy concentration of low cost TLDs, same three hosting providers used

for all. Similar HTML structure and page layout. Identical credentials harvesting flow. Thank you.

SARAH WYLD: Thank you, Francisca. Do we have thoughts? What would we do here? Is it DNS abuse? Do we think all of these 180 domains are part of the same scam? Brandon? Thank you.

BRANDON EASTHAM: Brandon, for the record. I'd nuke it from orbit. Thanks.

SARAH WYLD: It's the only way to be sure. Any other thoughts? I know there are some people behind us, if you want to come up and say anything. Again, our thought here is, is there sufficient association to suspend the other domains for DNS abuse? If we don't have discussion moments, we could do our show of hands. Do we have a yes? There is sufficient. I see several hands. We feel like this one's easy. I think so. Does anyone think no? I see a no. Would you like to speak to the no?

VIVEK GOYAL: Sometimes the cases are that the website faces defacements. And secondly, we also need to look at are the social names intellectually registered or not? We need to understand this whole framework and then take actions.

SARAH WYLD Thank you so much for that. Yes, sometimes we need to look for more information before we can determine how to proceed. Any other thoughts on our social scam before we move ahead? Michele, thank you.

MICHELE NEYLON I think the fact that the domains were registered within the clustered and batches thing as well, it's not a normal pattern in some respects. I mean, the kind of patterns we would see, kind of normal registration, somebody goes in and they register the same domain across multiple TLDs. Last night was hard, I'm still paying for it. Or maybe they do something again, a few days later, they come back and they register a bunch of domains related to some other concept. But doing them within short succession in weird kind of little bursts, it strikes me as a little bit odd. Now, to be perfectly honest, whether we would actually notice that or not is another thing entirely. I think a lot of this stuff here about the payment shopper account thing, I have no idea what the hell that is. And I don't think we would have access to that information. That might be something to do with whatever payment method this registrar uses. I don't know. I don't know what that is.

SARAH WYLD Thank you, Michele. I think it was PayPal, but I don't quite recall. Owen?

OWEN SMIGELSKI

Just to kind of counter what Michele suggested. Registrations and batches might appear to be weird for say, some people, however, there are certainly scenarios where that could occur, such as I put 15 domain names in my shopping cart and buy it. I purchase domains and batches sometimes. Or if you have a reseller model or somebody is acting as a reseller. Reg always told a story where she registers domain names for friends at a bar. All of her friends have a great idea and she puts them in a cart, so it looks like a batch. That's not always dispositive, but it depends as a good lawyer would say. Thanks.

SARAH WYLD

Thank you, Owen. It's not unheard of that a reseller would take orders throughout the day and then submit them all in one batch at the end of the day. That could lead us to this.

I think we already did our poll on this one. We're going to move to our final case file, the Case of the Nasty Network, and we will have Mohit read it again, please.

MOHIT KAMBLI

Nasty Network. In an extensive investigation targeting a large-scale fake web shop scheme, a registrar reviewed and validated over 10,000 domains to confirm their association and substantiate the claims of DNS abuse. Did they find a network or a nothing burger? Approximately, half of the domains identified as associated shared

the same registrant e-mail domain. Order time varied. Some of the domains were registered in a batch, others were registered in a 48-hour period, and others were registered over the month. The domains all used the same TLD. They were usually two or three random words, but not following a specific pattern otherwise. Payment source was mostly crypto using unique wallets, but with some PayPal for those purchases, the same identifiers were frowned across several accounts. The website all used the same template.

SARAH WYLD Thank you, Mohit. I see already we have someone determined it's a fake web shop scam network. If you'd like to speak to that, you're very welcome. What do we think? What are we doing with this network? I want to thank Volker for teaching me the word nothing burger. And please, go ahead.

VOLKER GREIMANN Normally, a fake web shop alone would not be DNS abuse, but yes, we'd nuke the entire network from orbit if it's the same registrant. If more than half of the domains are basically that registrant, then we'll take it down. Experience shows that in these kinds of cases, we never receive any feedback or complaints.

SARAH WYLD Thank you, Volker. Michele?

MICHELE NEYLON: Thanks. It might be a case of abuse. It might be a case of terms of service breach and we might do something, but I wouldn't see it as a case of DNS abuse. I don't know. Unless somebody else... Does somebody disagree with me? Volker? DNS abuse? Yes or no?

SARAH WYLD: As a reminder, DNS abuse is defined as phishing, pharming, malware, botnets, and spam e-mails when used to deliver one of those other types of abuse.

VOLKER GREIMANN: Well, like I said, normally I wouldn't say fake web shops are DNS abuse, but it says right there in the target that we have substantiated DNS abuse. As we have done that apparently, I would see that the facts of the matter have borne out that it is DNS abuse.

SARAH WYLD: I think that might just be a mistake in how I've written it. It's that they were investigating to see if it's DNS abuse.

MICHELE NEYLON: The question is, is there evidence to substantiate it? Not that it has been substantiated.

SARAH WYLD: All right. Thank you. Michele, your hand is still up. New thought? That's great. Thank you. What does anyone else think? All right. We'll do our final not quite Zoom poll. Is there sufficient association to suspend these 10,000 domain names for DNS abuse? Do we have a yes? Show of hands. We have some back there. Very good. Thank you. Do we have a no? I don't see any nos. Do we have some maybes in the room? I'm always a maybe. I see a bunch of maybes. Michele, please.

MICHELE NEYLON: It comes back to what I said earlier. I mean, I might suspend them, but it's not for DNS abuse.

SARAH WYLD: Thank you very much for that. Owen?

OWEN SMIGELSKI: Same thing as Michele and Volker. Definitely suspend, but not for DNS abuse. Other bad stuff probably.

SARAH WYLD: Thank you. Andrew?

ANDREW CAMPLING: Hi. Just to throw in at the end of the thing, maybe this is making the case for broadening the definition of DNS abuse. Throw that out there.

SARAH WYLD Well, there was some muttering in the room, as you said, that Andrew. I think perhaps my approach instead would be just because it's a bad thing that needs to be dealt with, doesn't mean it needs to be DNS abuse. Other bad things can also happen and be addressed in their own way separately. Michele, please.

MICHELE NEYLON Thanks. First off, no. The contract has requirements for registrars to deal with abuse reports. Abuse in that part of the contract is not narrowly defined. The base of the contract, which a lot of this is around, the specific DNS abuse amendments, which are very narrowly scoped. While yes, a lot of us would probably take action and do many, many things, expanding this scope of the DNS abuse definitions would cause more headaches than they would actually solve. And you would end up probably creating more headaches for everybody without actually solving anything. Be careful what you wish for. What you need to be looking at instead is instances of registrars not responding to abuse reports, which is a totally different conversation entirely. And if that's happening, please do report it to ICANN Compliance because I'm sick of getting audited when they get bored. Thanks.

SARAH WYLD Thank you, Michele. Volker?

VOLKER GREIMANN

I think the question of whether this is DNS abuse or not revolves around the question of what kind of fake shop it is. There are fake shops out there that are just shops that pretend to be the original, and therefore, still send out fake goods, as in fake shop for fakes. But there's also fake shops that pretend to be a shop and only exist to phish the payment details of the customers. Now, for us as a registrar, it's near impossible to figure out which one is which. I would say that the former category is probably not phishing and therefore not DNS abuse. This latter category is probably very much phishing and therefore DNS abuse.

As I do not care about making that definition, we are including in our terms of services that fake shops in general are not permitted, and therefore, we will take action on that basis. However, then you still have that can of worms, whether replica shops that clearly say that they are replica shops are still fake shops. Or if it's just the ones that pretend to be the original and then they'll send those fakes. There're all kinds of nuances and levels of fake shops and fake shopperies and asshattery going on in this space.

For us who only register the domain names and cannot see what transactions happen afterwards, it's very, very difficult to get to the bottom of that. And yes, we've had complaints where people had done trial shoppings on those stores to see what it was, but that's also something that I don't want to have right holders do in every single case because that obviously is a lot of work for them as well

and usually not worth the effort. For us, terms of service violation end of it.

SARAH WYLD Thank you, Volker. Vivek, please.

VIVEK GOYAL Thank you. I think Volker just mentioned the last word and solved my problem, but I'll still ask the question and the reason behind it. You clearly said that this is not DNS abuse, and so what is your incentive for taking this down? Because at the end of the day, once you take it down, you're losing business. What's the incentive other than they are violating your service agreement?

SARAH WYLD I think you've answered your own question. They're violating the service agreement. Thank you. As we wrap up, I see a couple more hands, but we're almost out of time. Just think about what have we learned? I've come away with two thoughts here. Number one, not everything that happens bad online is DNS abuse. And then number two, often it's unclear whether domains are associated or if they're used for DNS abuse. The investigation is very individual and contextual and complex. It is not always an easy problem. On that thought, we'll go back to Michele.

MICHELE NEYLON

Thanks. Just to respond to the gentleman who came up there a second ago. Terms of service stuff, generally, from our perspective is to protect the network in terms of the network's own reputation. We are a hosting provider primarily. We happen to sell domain names. The hosting part is the bit that pays my bills. If my network is flagged as being the source of crap, whatever form that may take, it becomes problematic for me. E-mails cannot be delivered. Other things don't work very well. It's a reputational issue at the network level. I'm talking literally at the protocol level.

Further up the chain, obviously it's also a question of whether you want to be associated with certain types of activity or whether you want to send a message to the broader Internet that certain types of activity just are not welcome. Like if you want to set up certain types of activity, don't come to us. We will shut you down and we will terminate with prejudice because we do not want certain types of activity anywhere near us. I have no problem saying that. I have no problem defending it. We have our terms of service. If you spam from my IP ranges, we will call your account. I don't care who you are.

VIVEK GOYAL

Very quickly, if you don't mind. 30 seconds. The reason for my question is because we are an online brand protection company and we file reports and we are very careful not to send crap your way and hoping like spray and pray because it reduces our reputation as well. And you mentioned term of service but I very

well remember I will not repeat that mistake told my team not to quote the term of service to companies again. Reg told us last time and I have said nobody write term of service. I don't want Reg's wrath. If I don't write term of service, this is not DNS abuse. So under what category... I know this is harm. It is harming us. The consumers losing money, the registrar's hosting providers doing money. How do I report it to you so you take it down?

SARAH WYLD

This is a good question. We need to take it offline because we are out of time. I'm so sorry that we didn't get to our last person in the queue but I have to wrap us up. But maybe that's something to come back to later. What do you do if it's not DNS abuse? Thank you.

Thank you so much, everybody, for your participation today. I hope you had as much fun as I did. I hope you learned something. If you need a copy of the slides there online, just let me know. And thank you. Have a great day.

[END OF TRANSCRIPTION]