YEŞIM NAZLAR: Good morning, good afternoon, and good evening to everyone. Welcome to the second At-Large Capacity-Building webinar on the topic “DNS abuse, an end-user perspective,” taking place on Monday 3rd of May, 2020, at 15:00 UTC.

We will not be doing a rollcall with the webinar. However, we will be noting attendance on the Wiki page. If I could please remind all participants on the phone bridge as well as computers to please mute your lines when not speaking to prevent any background noise, and also to please state your name when taking the floor, not only for the transcription purposes but also to allow for accurate interpretation.

Please keep your microphones muted at all times until we have the Q&A section. If you raise your hand the moderator will give you the floor. An important reminder to click on the chatbox to connect with other participants. For all questions, please use the format shown on the screen.

We have English, Spanish, and French interpretation, as well as real-time transcribing in English. You may find the link for real-time transcribing in the chat. Thank you, all, for joining. Now, I’d like to leave the floor to Joanna Kulesza, the co-chair of At-Large Capacity-Building Working Group. Over to you, Joanna. Thank you very much.

JOANNA KULESZA: Thank you very much, Yeşim. Welcome to the second Capacity-Building Working Group webinar. This time we would like to provide you with

updated information on DNS abuse and welcome you to a Q&A session regarding that very hot topic, especially in times of the global pandemic that is at times being used also for DNS abuse purposes.

Thank you very much to Hadia for setting up this webinar as a series of our Working Group Capacity-Building webinar section. Thank you very much to Jonathan for accepting the invitation to lead this week's webinar. Thank you very much to Drew for joining us and providing us with updated information on what DNS abuse is at this specific, unique point in time.

We welcome you to the webinar. We will try to follow the format that we've established this year in the sense of our speakers providing information, then posing certain questions we would like to hear your feedback on, and then possibly leaving us with a little bit of time for a Q&A session that will also welcome discussion. With that, without further ado, I would love to give the floor to Jonathan and our guest to start the DNS abuse webinar. Thank you very much, Jonathan. Over to you.

JONATHAN ZUCK: Thanks, Joanna. Thanks for the invitation and thanks, everyone, for joining. I've prepared a short video for my presentation so that I say "um" less often. Please enjoy. I'm available for questions at the end.

Good morning, good afternoon, and good evening. Or for the less fortunate, good middle of the night. Today, we're going to discuss DNS abuse, which has only become worse during the COVID-19 crisis.

We hear the term “cybercrime” a lot, but what’s DNS abuse? We’re all pretty familiar with the DNS, or Domain Name System, by now. It’s a fairly sophisticated system of questions and answers that gets you to where you want to go on the World Wide Web.

It’s a bit like a scavenger hunt where you need to ask one person for the name of the other person who knows the number of the person you want to reach. Of course, as they say in the movies, all that asking around can get you noticed by the wrong people. Just ask Dorothy as she asked around for wizard.oz.

Simply put, DNS abuse is a tax on, or the criminal use of, the DNS. Some people will try to parse this definition further by calling a tax on the DNS “DNS abuse” and a tax using the DNS “DNS misuse.” But for our purposes, we’re going to call it all “DNS abuse.” Now, we’re going to talk about different types of DNS abuse. Hey, what was that sound?

PRESENTER: It’s quiz time!

JONATHAN ZUCK: Quiz time?

PRESENTER: That’s right. You put them to sleep and I wake them back up. Your first question is, what is the DNS? Is it A, the Delaware Nature Society, B, the Division of Nuclear Safety, or C, the Domain Name System? If you choose C, the Domain Name System, you would be correct. To be fair, the

Delaware Nature Society and the Division of Nuclear Safety are DNSs, but not the kind we've been talking about.

JONATHAN ZUCK: One of the best-known attacks on the DNS is a distributed denial-of-service, or DDoS attack. Here, a perpetrator uses a network of zombie computers to make so many requests that a server is overwhelmed.

Sometimes, a criminal element gets in-between you and the servers from which you request information. This can be done with a so-called "man in the middle" attack, or a DNS cache poisoning. Simply put, the idea here is that your queries are intercepted and you're given the wrong number for the site you wish to visit.

The server-side redirect can be used for something called a "pharming attack," sometimes called "phishing without a lure." Here, you're simply redirected to a site that looks like the one that you intended but it's just set up to capture your log-in credentials. You think you're logging into your bank but really you're just filling in a form for hackers to go and use on the real bank website.

One of the most common abuses using the DNS is phishing, a far less technical way to get you to the wrong server is simply to ask you to go. In this case, you receive an e-mail suggesting something is up with your bank account and you need to log in to fix it. However, when you click that link you're taken to a pharming site. This process is called "phishing" because you are lured into the fraudulent site.

Here's an example of what such an e-mail might say. You can see that there are some key elements to such e-mails. Some kind of crisis with a short time to remedy so that you don't think about it too much and a call for you to log into your account. Of course, taking you to a fraudulent site isn't the only use of e-mails. Sometimes, they have attachments that contain malware directly.

One are of particular concern to the At-Large is Internationalized Domain Names, or IDNs, those domain names using non-Latin characters. These relatively new domains are essential to give the next four billion users on the Internet. 70% of the world uses non-Latin alphabets.

And finally, in 2012 we got the ability to register domain names in languages such as Russian, Arabic, and Chinese. Of course, with every new innovation comes matching innovation by the criminals, and IDNs were no different.

It turns out that a lot of letters in non-Latin alphabets look a lot like letters in Latin alphabets. Who knew there were so many ways to spell Bank of America? When someone sees one of these spellings while quickly reading an e-mail, why wouldn't they go ahead and click? In addition to collecting your credentials … What?

PRESENTER: That's right! It's time for another quiz. What is a denial-of-service attack? Is it A, when a waitress is upset with you, B, too many requests to a server, or C, coming to the store without shoes? That's right, it's B! Too many requests of a web server. Now, it's true that showing up to a store

without shoes might lead to a denial of service, but let's be honest – in that case, it's you who is doing the attacking.

JONATHAN ZUCK: In addition to collecting your credentials, these fraudulent e-mails and websites had a primary objective to plant software in your machine. This software is broadly called "malware" but there are many varieties of malware.

You've heard of these types of programs before and many of you, or your friends and family, have fallen victim to them, but we don't have time to go into each of them in detail today. Suffice it to say, whether it's spyware or ransomware, you don't want it on your computer.

Unfortunately, malware infection is on the rise. In the last ten years, malware infection has gone up nearly 700%. As an example, ransomware attacks have risen 350% in 2018 alone. In fairness, especially after the review of the 2012 round of TLDs for competition, choice, and consumer trust, the folks in ICANN Contract Compliance are doing their best. The compliance team began publishing more and more granular data about complaints and began to make its audit process a little less random. But it's still not enough.

You might have heard something called the "Domain Abuse Activity Report," which ICANN began a few years ago. While the monthly reports provide just enough data to know there's a problem, they don't provide enough to do anything about it, such as avoiding a domain or registrar that seems to be up to no good.

However, using DAAR we can determine that the percentage of infected abuse has gone down less than 1% since inception two years ago. So, we can all agree that DNS abuse is a major problem for individual users. But what can the At-Large do?

The At-Large will take a two-pronged approach to combating DNS abuse: outreach and ICANN policy development. The At-Large will develop education materials for end-users to better protect themselves against DNS abuse.

The At-Large is unique in its structure, making it possible to distribute information to the regional At-Large organizations or RALOs who, in turn, can distribute those materials to the At-Large structures, each of which have individual members to which they can finally distribute the materials.

The At-Large has been developing this network for years. What better use than to protect users from criminals on the Internet? There are a number of messages we can deliver to help people avoid the traps being set for them every day.

It's the enduring irony that criminals get most of the information they need from users not by being clever computer engineers but, like in the movies, by being clever social engineers. In short, if they want your password they basically just ask for it. This was true before the Internet and it remains true today. The At-Large need to educate users to be on the lookout for news that's too good or too bad to be true. There are always ways to figure out whether an e-mail is a fraudulent one or not.

We like to make fun of those phishing e-mails because of their bad grammar. What we don't realize is that bad grammar is intentional. Writing this way simultaneously triggers a deletion by those who recognize the scam and sympathy from those who are less sophisticated. The At-Large can certainly help end-users to discern the authenticity of an unexpected e-mail.

It should go without saying, but the At-Large will say it anyway, that individual users should have virus protection software on their PCs and mobile devices. In fact, in the United States, where you would expect considerable sophistication by users, nearly 50% of computers lack virus protection.

The At-Large must encourage end-users to ask their employers if they have DNSSEC-enabled servers to prevent events such as man-in-the-middle attacks. The other place the At-Large needs to be heard is in the hallways, meetings, and conference calls that make up the ICANN Policy Development Process.

The At-Large will engage in ICANN policy development at every point of entry. In one case, it might be a conversation in a hallway, or participation in a work group or review team. We will actively engage in advocacy for reforms both inside ICANN and among businesses that serve end-users such as registrars and registries. In other words, if someone asks us about the weather, we will stick out our hand, look up at the sky, and say, "It feels like DNS abuse."

Thankfully, we're not alone. The majority of the ICANN community is concerned about DNS abuse and hesitant to allow a new round without

significant reform. There is simply no way that a minority of voices should be able to drive ICANN to a new round without real buy-in from the rest of the community.

The At-Large has and will continue to partner with other groups within the ICANN community to sound the alarm regarding DNS abuse and actively promote reform. Our first task is to simply hold the line. There should be no new round until DNS abuse is addressed in a meaningful way.

Compliance needs a holistic view of DNS abuse. It cannot simply react to complaints but must use their audit power to recognize high percentages of abuse and take action against TLDs, registries, and registrars who are part of the problem. We need to limit volume registrations because there is a high correlation to DNS abuse.

Of course, there are legitimate uses for bulk registrations and such uses will only increase with the Internet of things. But the At-Large will continue to advocate for increased friction for such activity, perhaps requiring authentication as a legitimate bulk registrant.

The CCT Review Team, and consequently the Security and Stability Review Team, have both suggested that ICANN design incentives to adopt best practices. The At-Large will continue to advocate for such incentives. Certainly, more research can be done and has been recommended by the CCTRT, the SSRT and the ALAC, and now Verisign. There are now, essentially, 20 million dollars more in the budget to invest in security and stability of the DNS.

There are certainly those registries and registrars that are investing significant time and money in combating abuse. In fact, 48 companies have signed onto a commitment to best practices. That's awesome, but we still need reforms to better address the bad actors. And frankly, even the good actors could be doing better, so the At-Large won't be easing up on those guys any time soon, either.

It's like that old Dilbert cartoon in which we're reminded that once everyone has adopted so-called "best practices" those practices become the new normal and are no longer the best. The criminals are not satisfied with the status quo, and neither can we afford to be. So, even the good guys can do better.

All that is to say that this is a crisis from which no one is immune. Incredible research is happening in machine learning to better detect abuse in real-time and to predict that a registration is intended for illegal use. Early tests of such technology by .eu show a nearly 80% accuracy in such predictions. We need to ensure that such research continues and systems are put in place to protect us from the next generation of attack.

PRESENTER: That sound means it's time for your last question. Which of the following are tools to combat DNS abuse? A, education, B, implementing DNSSEC, or C, end-to-end encryption? If you chose all of them, you are correct. If you didn't, please stay after class.

JONATHAN ZUCK: When all is said and done, there is really only one constituency – end-users. It's the interest of those end-users the At-Large was created to advance. DNS abuse affects all of them. Say it with me: we have no use for DNS abuse. Go to at-large.wiki/dnsabuse for more information. Thank you.

Thanks, everyone. I'm happy to take questions at this time if you have any before we move onto Drew. Seeing none, I don't think. Let me scroll up here. Staff, have you identified any questions in chat? I didn't see any go by. There is a question. Yes, go ahead.

YEŞIM NAZLAR: Sorry, Jonathan. I was just going to say that I'm not seeing any questions in the format that we have for participants to use.

JONATHAN ZUCK: Okay.

YEŞIM NAZLAR: I'll scroll through as well, just in case. Oh. Actually, we see one question from Raymond Mamattah.

JONATHAN ZUCK: I see it. I see the question. Yeah, the question is about pharming and whether it's a normal term or one of my creations. I wish it was my creation because it's a good expression but it is, in fact, a good general term that you should be able to find references to around the web.

One of the things that we plan to do as At-Large is develop the DNS abuse page on the Wikipedia because, right now, there hasn't been one on DNS abuse. And so, we're hoping to develop out that page and make sure that people are able to see the DNS-centric part of cybercrime. That's what we refer to as DNS abuse.

So, DNS abuse is kind of a subset of what we often think of as cybercrime because there are some types of cybercrime that aren't DNS abuse. All right? Okay. So, Drew, I'm going to hand the microphone over to you.

DREW BAGLEY: Thanks, Jonathan. Would you like me to share my screen so I can move the slides?

YEŞIM NAZLAR: Oh, sure. Absolutely, Drew. Just give me one second, please.

DREW BAGLEY: Okay. Thank you very much.

YEŞIM NAZLAR: The co-host slide.

UNIDENTIFIED FEMALE: Glenn had a question in the chat.

JONATHAN ZUCK: Yeah, I see it, Glenn. I'm not sure I understand the question. “Do you see a spike in COVID-19 term phishing?” In other words, is there a spike in phishing for COVID-19? Is that the question? Because there is certainly a lot of it and that’s exactly what Drew is going to be talking about. So, if your question hasn’t been answered at the end of Drew’s presentation then bring it up again.

DREW BAGLEY: Thank you. I know that I know many of you and have had the opportunity to address many of you before, but for those of you for whom I’ve not met, my name is Drew Bagley and I help lead a non-profit organization called The Secure Domain Foundation, which focuses on tackling DNS abuse. I'm also the Vice-President of Privacy and Cyber Policy at CrowdStrike, which is a global cybersecurity company.

And so, with those perspectives in mind, I put together a presentation today to brief you all on what we’ve observed with some of the latest threats related to DNS abuse in the context of COVID-19, as well as going over some of these concepts that Jonathan explored in that “Introduction to DNS Abuse” video, so that you can get a better sense of means to identify and tackle DNS abuse in context.

So, some of the trends that have been observed over the past two months, since the COVID-19 pandemic has swept the world, had been that bad guys are, obviously, taking advantage like they do of any situation of, of course, this situation.

And so, interestingly, there are a couple of trends going on right now where the dynamics by which people are vulnerable are a bit different,

both from a social engineering perspective as well as even from a technical perspective.

Because depending on your location, your industry, and what your local government authorities may be requiring in terms of stay-at-home orders and whatnot, there is a multitude of work situations going on right now where you have organizations that, maybe, were able to roll out corporate devices for work from home. And you have other situations in which people are using their own personal devices to work from home.

And so, that environment alone, where you have less control over cybersecurity and data, coupled with this sense of all of us trying to seek as much information as possible about COVID-19, has led to this environment where adversaries are attempting to design phishing attacks and other sorts of attacks that take advantage of people trying to look for COVID-19 information and taking advantage of the fact that people might be utilizing personal devices on which they're not running any sort of end-point security or may not have any firewall in place and whatnot.

And so, what that has led to is several cyberattacks where domain names have been registered incorporating COVID-19 as a term, or World Health Organization, or the acronym WHO, or the Centers for Disease Control, CDC, and other variations, and plays off of that, and attempts to pose as legitimate websites or to pose as legitimate servers from which e-mail is coming from. And so, there have been a lot of campaigns doing that. And so, I'm going to show you a few examples from around the globe.

So, here the Australian Signals Directorate, their Australian Cyber Security Centre has been warning people about a campaign that has been targeting those geographically based in Australia. And so, this campaign involved the registration of a domain name, covid19-info.online, in this case utilizing a new gTLD, and was sending texts messages, sending SMS messages, rather than e-mails, to try to get people to click on a link from their mobile devices, and this link could be used to deploy malware.

Similarly, there have been other campaigns that are very, very similar, such as in the UK where there was this domain name, uk-covid-19-relieve.com. In this instance, this domain name was trying to get people to click on a domain name to go to a website in which victims would input information like their passport information and other personal information that then the cybercriminal would get a hold of for further identity theft, financial crime, and other sorts of thing.

And so, you can see in both instances we have—and let me just even go back a slide—the WHOIS information here that shows you that these domain names were registered very recently. So, oftentimes, when you're trying to gauge the authenticity of a domain name you're paying attention to several variables, one of which would be when a domain name was registered.

Here, of course, the global pandemic itself is a recent event. So, that alone might not be indicative of this on its own being a suspicious domain name. But if you look further, all of the registration information is hidden behind a proxy. This one is WHOIS Guard, which is based in Panama.

And so, that's something where when end-users are attempting to understand whether or not a domain name is legitimate, obviously, as Jonathan was alluding to, you really need to scrutinize the message itself.

But then, you can even do follow-ups on the domain name by utilizing WHOIS. And if all of the details are hidden, that may or may not be indicative of whether or not something is suspicious, but it's certainly something to keep in mind and ask yourself whether or not that's something you trust. And so, you can see that in both instances, here, as the common thread with these domain name registrations.

And so, I do not have the wonderful theme music that Jonathan had. But with that said, to prevent you from falling asleep, we're going to have the first quiz question. So, the quiz question is, "It's easy to tell if an e-mail is legitimate. True or false?" I'll give it five more seconds. I see everybody being pretty active. All right.

And the correct answer is "false." It really isn't always easy to tell because social engineering really is a true form of art at times. And so, adversaries can really even be very specific in the way that they're fine-tuning something if they know someone is associated with a certain organization. It might be expecting a certain type of communication. Or even in terms of trying to cover their tracks with things such as spoofing their WHOIS registration information or things like that, and even spoofing the address that an e-mail comes from.

So, I'll show you an example of that. Let me share the results with you of the poll real quick. So, you can see that more than half of you guessed "false," guessed correctly, but some of you thought you might be able to

tell. Let me just show you an example of an e-mail where this wasn't the case.

So, here you can see that the e-mail purports to come from what is a legitimate domain name, who.int, as well as even a legitimate e-mail address. If you look up at this e-mail address, this is a real email address associated with the World Health Organization.

Similarly, there have been campaigns—not only the one pictured but other campaigns that have gone on in the past two months—that have incorporated other legitimate WHO [inaudible]. So, eurohealthcities@who.int, as well as donate@who.int.

And so, in these instances, the e-mail itself appears to be coming from these e-mail addresses even though it's not. And so, the return address in the e-mail is actually being spoofed.

There are various ways that organizations can prevent these sorts of things, by tightening the security on their e-mail servers themselves so their e-mail servers can't be utilized for these things, or deploying certain technologies like DMARC and whatnot.

But nonetheless, this is a very common occurrence where e-mails can be spoofed in such a way. Sometimes, maybe an adversary would not be successful with actually spoofing the e-mail headers but, nonetheless, the body of the e-mail could make the e-mail appear as if it came legitimately from the organization by loading real graphics and other links that are associated with the legitimate organization.

So, this is just a great example of why it's not always easy to tell the difference. And so, if you want to see more examples of these sorts of campaigns then I recommend you check out the blog that's linked to at the bottom of this slide.

So, some tips for staying safe. Building off of what Jonathan was talking about a few moments ago, it's really important whenever you're receiving an SMS, or an e-mail, or any other form of communication that has any sort of link or is requesting that you do anything, you take an action with money, or you send some information back, or anything like that, it's really important that you scrutinize the whole picture and to stop, think, and connect.

And so, first of all, of course, like I was suggesting, inspect the e-mail headers. But as you can see from that last example, that alone might not tell the full story. Try to use WHOIS to determine whether or not a domain name registration looks legitimate or not.

And again, another tip with that is, if everything's hidden behind proxy, that might be an indication that it might not be legitimate. On the other hand, sometimes legitimate domain names also use proxy registration. But again, consider the totality of the circumstances, here.

And then, also think about whether or not whoever is contacting you is someone you might be able to try to call or contact some other way to see if the e-mail really did come from them, if it's legitimate. Or even rely upon, in the case of the WHO examples, the organization's website to see if they have warned about any such phishing scams.

In the cases that I have presented out of Australia, the United Kingdom, and with regard to WHO, in all three cases, the government or international institution websites have warnings about these alerts after these alerts have been discovered. So in these cases, the domain names have not yet been taken down. People were still being scammed but the organizations themselves were at least warning people. So, always look out for that.

And then, make sure that you're protecting your devices with an effective endpoint protection solution. This is really important. It's really important to find cybersecurity solutions that really focus on evolving threats and aren't requiring you to do updates and patches every single day but that that are automatically doing those sorts of things for you and focusing on what adversaries may be doing even without malware or whether or not your computer is being redirected to places that it shouldn't be redirected to. So, it's important to be thoughtful about that on your personal devices, as well as with your own organization.

And then, if you're a member of an organization, it's really important to provide cybersecurity training, especially during these times in which people might have very unique, remote work situations, which can open up a whole threat factor to individuals as well as to organizations.

And then, similarly, another way to test URLs or files is to utilize one of the free online [multi-scanners]. And so, the way those work is that you can use sites such as the example I gave, hybrid-analysis.com, and you can paste the URL and see what it would have done to your computer, or a file. And so, there are several free ones out there that you can explore, and those can be helpful. So, that way you're testing it with the

cybersecurity site before you would actually run it on your own computer.

And now, time for quiz question two. What's an example of proactive anti-abuse, that'd be proactive in combating abuse? I'll give it about 15 more seconds. Okay. Final answers. I'm about to end the poll. It looks like maybe the … Okay. You have the results up. Yeah.

So, the example is both C and D, here. So, if you're doing something after it has already been used for something bad then that would be reactive anti-abuse which, of course, in the example that I just showed you with those domain names, it's very important after something is discovered to make sure that the domain names are being suspended and that, maybe, even an entire account associated with a domain name is being looked into to see if there are other domain names being used to perpetrate DNS abuse and cybercrime.

But there are activities such as what Jonathan alluded to in the intro to DNS abuse where you can actually identify suspicious domain names before they've been used. You can look for certain characteristics that might be associated with phishing campaigns, such as some of the bulk registrations and whatnot, and add friction to that process.

Similarly, if a certain registrant account has already been associated with known DNS abuse, such as phishing sites, DNS hijacking, or anything else, then that's something where you could introduce a layer of friction before that registrant is able to add more domain names to their account in the event that they're just adding domain names to be used for those purposes and aren't a legitimate user that has actually been hacked.

And so, these are the results. So, not bad. Not bad. So, what's interesting about encouraging parties to partake in proactive DNS abuse is that there are actually a lot of incentives that are aligned for end-users, who could be would-be victims of DNS abuse, and organizations that run businesses that control Internet infrastructure.

That's because DNS abuse really isn't good for anyone—except for the cybercriminals—because, whether you're a ccTLD or gTLD registrar, then there is pressure to respond to complaints. That takes up time and time, of course, is money with the business.

That can add friction to your operations and what you're able to do as a business, as well as, if you're not complying, potentially put you under the microscope with regard to authorities, and even your overall reputation and whether or not a business would want to do business with you if you're not regarded as being a clean place to do business.

In the case of a registrar or even a registry, there can be entire TLDs where a business might decide they don't want to register a domain name with a certain TLD because they always see scams ending in that TLD and they think no one will take their own domain name seriously.

And then, similarly, when you're reactive with anti-abuse and you're one of these organizations, then you have to worry about suspending domain names after the fact, potentially credit card charge-backs, or even court orders, or lawsuits, or anything like that. And so, that's why it's very important, really, to encourage everyone to be proactive with anti-abuse.

But nonetheless, what we see now in this current climate with COVID-19 is that domain names that are very easy to identify as spoofing

international organizations, like WHO, or incorporating COVID-19, are nonetheless successfully registered, added to the DNS, and then used. And so, this is something where even though there are these incentives lined up, maybe best practices aren't being adopted to identify these things beforehand and scrutinize them early on before they're able to be used to actually inflict harm on people.

Which brings us to quiz question three. Who is affected by DNS abuse? All right. I'll give it about 15 more seconds. Okay. I think we got some good feedback. All right. And you guys did fantastic on this one. If you guessed "everyone," you are correct.

And that's the thing. I think that even the discussion about financial incentives for businesses that run Internet infrastructure really spells out that they're affected, too, in addition to all end-users who could be would-be victims, and organizations that employ end-users, where something as simple as clicking on a link could actually pose a really significant threat to the operations of an important organization such as a hospital.

If you think about some of the attacks we've seen over the years with ransomware spreading, with [inaudible], and with other attacks—even supply chain attacks like the CCleaner supply chain attack from years ago, and WannaCry—really everyone can be affected by something as simple as a DNS registration that was registered for abusive purposes being successfully used to deploy and deliver some sort of malware. Or it could be used to harvest personal data from people and cause personal data breaches. So, this really is something that can be used to affect everyone.

All right. We're going to move onto the next poll. Or the next question, rather. Who has the ability to prevent DNS abuse? I don't know if that quiz question is displaying properly so I might need help getting that displayed.

YEŞIM NAZLAR: I don't see the tab to do it. The poll is not showing up.

DREW BAGLEY: There we go. Okay. I'll give that about 15 more seconds. All right. For all of you who said, "We all do," that's correct. ICANN as a community, as well as ICANN as an organization, has a big role to play.

The contracted parties are on the frontline of defense sometimes with these situations in potentially being proactive and flagging a registration before it's used to do something bad, or in assisting after the fact to ensure that a phishing campaign or some other sort of campaign is stopped – end-users, in identifying and reporting these threats, as well as protecting themselves and ensuring that cybersecurity is at the forefront of their thinking when they're clicking on things, as well as the cybersecurity community in analyzing these sorts of things, and warning the public, and in implementing safeguards into cybersecurity software to protect users.

And so, ultimately, Internet governance is very important for combating DNS abuse. That's why, as Jonathan articulated, the At-Large community really plays a unique role in representing end-users and in ensuring that,

ultimately, end-users have a voice in explaining, educating, and even promoting policy solutions that can really have an impact on DNS abuse.

And so, that's where, whether it's ALAC or other parts of the ICANN community, ICANN as a community can really create incentives for all the parties to ensure that where there is this common ground, and that DNS abuse is bad for everyone and is also something that everyone should do their part in combating. That really the community does that, such as by undertaking proactive anti-abuse measures, providing incentives to really be more actionable about DNS abuse, and to find ways to prevent some of these really simple examples I shared with you today.

From being able to happen as easily in the first place, where you can spoof COVID-19, WHO, and CDC in domain name registration and successfully use those. That's something that, hopefully, should not be able to happen. And so, that's where this constituency and the ICANN community as a whole really can play an important role and an impactful role in combating DNS abuse.

And with some of the things that Jonathan mentioned such as DAAR, as well as other data that's out there from a cybersecurity community, there really is, now, a time where a data-driven approach to this can be used. Because there is data that indicates how this DNS abuse is perpetrated, which registrars and resellers are used for registrations of certain domain names, which zones tend to host abusive domain registrations for longer periods of time. And so, that's where it's important to, now, take this data, and actionalize it in Internet governance, to do something about DNS abuse.

And so, the quizzes are over but I just have a couple poll questions for you. So, the first one is just, have you been targeted by COVID-19-related phishing campaigns? They don't necessarily have to be the ones I showed, but just anything, by SMS or via e-mail. I'll leave this poll up for about 15 more seconds.

JONATHAN ZUCK: Just to note, there are two questions in this poll, so everyone should scroll down and answer both questions.

DREW BAGLEY: Oh, yes. I didn't realize they were on the same poll. Yeah. The second question in the poll is, have you received additional cybersecurity training from your employer since the COVID-19 pandemic began? Okay. I'll give it about five more seconds [still be] answering.

UNIDENTIFIED FEMALE: Hello? Hello? Hello?

JONATHAN ZUCK: Hello?

DREW BAGLEY: Hello?

UNIDENTIFIED FEMALE: Hello, [inaudible] on the screen?

DREW BAGLEY: I'm sorry, what was that? Hello?

UNIDENTIFIED FEMALE: Hi, [inaudible] on the screen. Can I just answer now?

JONATHAN ZUCK: Sure.

UNIDENTIFIED MALE: She said, “Is there something shared before your slide at the screen?”

DREW BAGLEY: Oh, yes. There is, yes. There are two poll questions being shared. But we just ended the poll, so now we’re going to share the results. So, it looks like, unfortunately, a third of you who responded have been targeted by COVID-19-related phishing campaigns. Some of you don't know if you have, and then more than half of you believe that you have not been.

And then, it looks like only a quarter of the respondents have received additional cybersecurity training from their employers since the pandemic began. And so, that’s something where, for the reasons I stated at the beginning of the presentation, I think that’s really important right now.

Because oftentimes, the remote work arrangements are looking a little different, where employees can be connecting to corporate

infrastructure from personal devices, or just using personal devices for work and whatnot, and might not have some of the safeguards that are in place in an office environment for work or just, even if none of that has changed, might not be aware of the ways in which adversaries are using this latest pandemic in attempts to target people.

And so, that's where I think that's really important. If you are able to have that influence in your organization, to help people and help direct people to more training, then that's a really important thing to do.

So, that's the portion of my presentation in all of this but I'm happy to look at any questions that may have popped up during the presentation. I was not looking at the chat at the time.

JONATHAN ZUCK: Sorry, Drew. I'll ask them for you. There were several questions that came your way. One is that we usually see that registrars are not responsive to requests for information. Do you have any examples of when registrars or registries have been helpful in resolving these issues?

DREW BAGLEY: So, yeah. I'd say that's happening all of the time. Both situations are happening all the time. So, registrars and registries, it really depends on which registrar or registry and sometimes it depends on the circumstances and how much attention that certain domain name has gotten as far as how responsive they might be.

I have certainly heard about that, though, where you do have situations where parties still aren't being responsive, nonetheless. And so, I don't

have a specific example to share as far as where they have been responsive but I know that we definitely see that with my organization when we're trying to tip off certain registries and registrars to cybercrime we're seeing. It really just depends on the party and sometimes they're being very responsive.

However, being responsive after the fact is great and important but that's not the same thing as finding ways to be proactive with anti-abuse when a registration first pops up and before it's actually used to harm individuals. So, I would just say that in those instances it's really important for people to be persistent if they're needing to file complaints with registrars and registries, to help alert them to abuse.

Sometimes, it might be important to get ICANN Compliance involved if the registrar and registry is not complying with their obligation, and not investigating, and not being responsive, but that in the bigger picture a lot of those recommendations that Jonathan alluded to from the CCT Review Team, on which I served with Jonathan, a lot of those might really need to be implemented to get incentives in the right place, to get these parties to be more proactive.

JONATHAN ZUCK: Thanks, Drew. Another question, from Samridh Kudesia: "I didn't quite understand how the information in the headers can be different from the other fields, like [Chrome] field, etc. Can you explain how that works?"

DREW BAGLEY: Sure. That can happen in a variety of different ways, but one way—depending on how a server is configured—is sometimes an outgoing e-mail server is not configured with the same security as an incoming e-mail server.

And so, a person not affiliated with a certain organization could just put in the outgoing e-mail server details of the organization they're wanting to spoof, and not even need any credentials, and would be able to ping that server and make it look like the e-mail was coming from that server. That would be one way.

Sometimes, instead, what adversaries are doing is they're actually not utilizing a legitimate server. They're making the header appear that it's coming from the legitimate server by registering a domain name that looks nearly identical to the legitimate organization. So, they might be able to use two Vs instead of a W, or something like that. So, it can really vary. Sometimes, they're really able to actually utilize that outgoing e-mail infrastructure if an organization doesn't secure their e-mail servers properly.

JONATHAN ZUCK: Yeah. Thanks, Drew. Same thing, I guess, goes for some of those IDN homonyms, as well. All of those different spellings of Bank of America looked exactly like Bank of America but they were just using non-Latin characters.

DREW BAGLEY: Yep, exactly.

JONATHAN ZUCK: Okay. This question from Gopal Tadepalli: “We do not make 100% foolproof systems. What is the support from ICANN in analyzing a breach/incident response? More so when 70% of such threats are internal to the organization.”

DREW BAGLEY: So, I think that organization might be more directed for ICANN Org with regard to what they would do in the circumstance of a breach. Again, ICANN Org—whereas data breach is merely utilizing the DNS but impacting other organizations—are going to really involve a multi-pronged approach where organizations might want to have incident response services on retainer or know who to call if they are breached.

And then, ultimately, you really have to stop the criminal infrastructure. So, you really have to figure out where domain name are registered, where IP addresses are pointing back to and being hosted, and whatnot, and make sure that that infrastructure is being taken down in the case of a breach. But as far as how ICANN Org itself would respond, and does respond, to threats to its own internal organization, that would be better directed at ICANN.

JONATHAN ZUCK: Thanks, Drew. This is from Hadia Elminiawi: “Does the lack of public domain name registration data have a negative impact on DNS abuse?”

DREW BAGLEY: I believe it does from a cybersecurity perspective. So, one of the things that we see in the cybersecurity community is that it's much more difficult to do correlation analysis. So, whereby, before, even if you had bogus information in WHOIS, as long as you had some form of common bogus information, like a common e-mail address being used, you could then query off of that e-mail address to find other registrations associated with that e-mail address.

So, you might find that while there is one domain name already known to be used for some sort of malicious behavior, if you query off that e-mail address you could find 100 more domain names registered around the same time that haven't yet been used but that you have a suspicion would likely be used because they're associated with the same registrant. Whereas now, with WHOIS going dark, that correlation analysis is very difficult to do because there is a lot less data to do those pivots off of.

And with that said, the use of proxy services for privacy has been there for years and years. But one of the differences is that, depending on the cybercriminals, cybercriminals weren't necessarily always using those proxy services. So, that's where they might be putting their bogus details in the public rather than paying the extra money for the proxy. And then, that would cybersecurity researchers that extra correlation information.

JONATHAN ZUCK: Thanks, Drew. Next question: "Are there free applications to test for end-point security in malware that are available and you know of?"

DREW BAGLEY: Sure. One of the web-based ones that I referenced in my presentation is hybrid-analysis.com. And so, what that is is it's a platform that runs cybersecurity sandboxes. So, you can put a URL or upload a file and it will actually test it and generate a public report. So that way, everyone knows whether or not something is safe. It can help alert people to scams and it will show you screenshots of what it would have done to your computer. So, that's one, and then there are several others out there, too.

JONATHAN ZUCK: Great, Drew. Thank you. "Couldn't DNS abuse be commercial espionage?"

DREW BAGLEY: So, DNS abuse can be leveraged for all sorts of things. So, you could have state actors, which we've seen levers the Domain Name System for whatever their interests may be. You have e-crime actors using it to defraud people. You have hacktivists using it, potentially, to disrupt things and whatnot. And so, DNS abuse could be used for virtually anything. Any instance where you're abusing the Domain Name System to carry out something that's not permitted could fall into that category.

JONATHAN ZUCK: Thanks. And then, this is another one that might be an action item for staff. This question from Vivek: "What is the contractual response time for a registrar/registry to avert on a complaint? Is the data about how many complaints were received and how they were resolved by a registry/registrar publicly available?"

DREW BAGLEY: Yeah, I would defer to ICANN Org.

JONATHAN ZUCK: We'll take that as another action item and post the response on the CPWG and also on the Wiki page for this webinar. And I believe that is all of the questions. Thanks so much, Drew. Back to you, Joanna.

DREW BAGLEY: Thank you, Jonathan.

JOANNA KULESZA: Thank you very much, Jonathan. Thank you very much, Drew. That was most interesting. I really appreciate the fact that we managed to link this to the current situation. Thank you to everyone for the questions and the feedback. I'm wondering if there is anyone who would like to provide feedback in audio as opposed to the chat, or are there any comments that we might have missed?

I see a comment coming from Gopal: "Thank you for answering my question. Is there an upper bound on the time spent via message within the organization?" I would assume that question might need a follow up from Gopal as it stands.

I'm wondering if there is anything that we might have missed, if there are any hands up coming on the floor. I don't see them. I'm wondering if Drew or Jonathan might want to take a stab at that question as it stands

on upper bounds in the time limit spent via message within the organization. I'm not sure I get the details of that but maybe that is easier for our presenters to answer than it would be for me.

JONATHAN ZUCK: I think that's another ICANN question. So, we'll record that question, as well, and make sure that we get an answer to it on the CPWG list, as well as the Wiki, for this webinar for folks that are not familiar with the CPWG.

JOANNA KULESZA: Perfect. Thank you very much. Indeed, this webinar, capacity-building webinars, are indeed to serve as an initial step to getting involved in policy and getting a better understanding on all the issues that are related to DNS abuse and policy-making within ICANN. I'm wondering if there are any other comments or questions coming from the floor?

I believe we still have some time left with regard to the original timing for this webinar. A question from Vivek: "Has the DAAR report enabled any proactive DNS abuse action?" Guys, I'm wondering if you have any specific responses on that? I'm not sure how deeply involved you are with DAAR feedback.

JONATHAN ZUCK: Drew, you might want to take this, but right now the one piece of information that's missing from DAAR is the actual name of the contracted party that is currently in violation. And so, it's difficult for those outside of ICANN to use DAAR for proactive enforcement, and that's one of the things that the At-Large has been advocating for, which

is to make that information available sooner, like the actual name of the registry or registrar that's misbehaving, so that folks can make a proactive decision to stop doing business with that particular contracted party.

DREW BAGLEY: Yeah, that's absolutely right, and that's something where, if you look at the CCT Review Team report, one of the things that we really emphasize is taking a data-driven approach to this problem. And so, that's something where—whether it's utilizing the DAAR data or utilizing other data that's out there, because the cybersecurity community regularly publishes information, too, that could be actionable—that mechanism for taking action and utilizing data really hasn't been there.

JOANNA KULESZA: Thank you very much, Jonathan. Thank you very much, Drew. My understanding is that this is, indeed, a stepping stone, so to speak, on providing tangible feedback on the policy. So, the information the participants—and once again, thank you for taking time to join us—are receiving here is indeed a stepping stone toward making the DAAR or, effectively, this higher Policy Development Process as effective as we can make it. There is a feedback report we would like to have from you in terms of how effective you have found this webinar or this series of webinars to be. I understand that Yeşim has the questions. Is that correct, Yeşim?

YEŞIM NAZLAR: Hi, Joanna. Yes, correct. If I may, I would like to display the evaluation survey questions.

JOANNA KULESZA: Yes, please go ahead. Thank you very much.

YEŞIM NAZLAR: Okay, sure. Thanks so much. So, we have seven questions. If you can please take a couple of minutes to answer these questions, they are really important for us. I'm going to read out the questions for you, also.

Our first question is, how did you learn about this webinar? Please note this is a multiple-choice question. Twitter, Facebook, At-Large mailing list, At-Large calendar, Skype, a colleague, or others. You can choose as many answers as you like.

I'm going to move onto the second question as you are able to read all the questions. What region are you living in now? Is it Africa? Is it Asia, Australia and the Pacific Islands? Is it Europe? Is it Latin America and the Caribbean Islands, or is it North America?

Our third question is, how do you feel about the timing of the webinar? As you know, it was at 16:00 UTC, the start time of this webinar. Do you find it too early, just right, or too late?

Slowly moving onto our fourth question, did the webinar duration allow sufficient time for the questions? This is a “yes” or a “no” question. Our fifth question is, “The presentation was interesting.” Do you strongly agree, agree, neither agree nor disagree, disagree, or strongly disagree?

Slowly moving onto the next question: “I learned something from this webinar.” Do you strongly agree, agree, neither agree nor disagree, disagree, or strongly disagree?

And here is out last but not least question. “I would like to participate in other At-Large webinars.” Do you strongly agree, agree, neither agree nor disagree, disagree, or strongly disagree?

I'm going to keep the poll open so you can take more time while answering the questions. This is the end of the evaluation survey, Joanna. Back to you. Thanks so much.

JOANNA KULESZA: Thank you very much, Yeşim, and thank you to everyone for participating, for providing your responses. This will allow us to make the webinar better, hopefully, to better attend to your needs and your interests. My understanding is that there are no more questions. There are the questions. And there is no more feedback.

With that, I will slowly be wrapping up. Please let me note that this webinar subgroup of the Capacity-Building Working Group is led by Hadia, who joined us here today. Thank you again, Hadia, for scheduling all the webinars. Thank you for inviting our speakers. Special thanks to Jonathan and to Drew for taking the time to lead us through the ever-changing DNS abuse landscape.

We sincerely hope that this will allow us to get you more involved in policy development. DNS abuse, as Jonathan rightly indicated, is of crucial importance to end-users across the globe. With that, we hope that you

will use the knowledge or the update that was provided here today to get more involved in policy development. The website and the meeting times for the Consolidated Policy Working Group have been shared here.

With that, let me just note that there is another Capacity-Building webinar scheduled for July 1st. We will be speaking, in a sense, again about cybersecurity but we would like to give this a more general focus as opposed to DNS abuse in terms of domain names and [sent messages]. We would like to discuss geopolitics and the position that the Multistakeholder Policy Development Process within ICANN holds in today's political landscape or diplomatic landscape, so to speak.

I'm very much looking forward to moderating the webinar on July 1st. You will be provided with more updates as we move on. Hopefully, we will have a position from the board. We will have an end-user perspective during that webinar and I'm also very much looking forward to updates from ICANN Org on the work that is being done on the ground in day-to-day policy development and diplomatic relation.

As Heidi notes here in the chat, the first is on June 1st. It is June 1st at 20:00 UTC. I apologize if I misspoke there but you will have updates coming on the mailing list.

With that, I would like to thank our speakers again, thank everyone for participating. Thank you to our language services. With that, the meeting is adjourned. Thank you very much, everyone.

YEŞIM NAZLAR: Thank you all for joining today's webinar. This webinar is now adjourned.

[END OF TRANSCRIPTION]