ICANN84 | AGM – ccNSO: TLD-OPS Work Session
Sunday, October 26, 2025 – 10:30 to 12:00 IST

CLAUDIA RUIZ

Hello and welcome to the ccNSO TLD Ops work session. My name is Claudia Ruiz, and I along with my colleague, Joke Braeken, are the participation managers for this session. Please note that this session is being recorded and is governed by the ICANN Community Participation Code of Conduct, the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy. Please observe the following guidelines to participate in this session. I will also put them in the chat for your reference. During this session, questions or comments submitted in chat will be read aloud if put in the proper form as noted in the chat. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will unmute their Zoom microphones, and on-site participants will use a physical microphone to speak. For the benefit of other participants, please state your name for the record and speak at a reasonable pace. Thank you. And with that, I will now hand the floor over to Regis Masse, Chair of TLD Ops. Thank you.

REGIS MASSE

Thank you, Claudia. Hello, everyone. Thank you for joining us this morning on Sunday morning. This session is a small workshop for TLD Ops. It's about security. It's not a training session. It's just to give some information and open mind about security issues and

what we can do together to about cyber security attacks for ccTLDs. Just for those who don't know yet, TLD Ops is group that has been existing for a long time ago now, but it's a way to share contacts between the ccTLDs and sharing information about security. And we have done different things. We have done deliveries. We have gone TTX during some other ICANN meeting. And today with the group, we are trying to present you some elements of cybersecurity. As I said, it's not a training. It's an interactive, I hope, session with the room about security stuff. And the idea is to show open-source tools that you can use if you don't know them yet, just thinking that security is everywhere, every day, in jobs. So the main objectives of this workshop is to raise awareness about threats, talking and sharing real world examples to explain that and provide practical open-source security tools. In the webpage of the TLD Ops group on the ccNSO webpage, you've got already a list of tools, open-source tools that you can use to analyze and to prevent security attacks. And the idea of this workshop is to talk about just security. So I will share the mic with my colleagues, of course. But we've got an agenda for this session. So I will do a small introduction and context just to share the context of security for ccTLDs. And then we talk about threat landscape for registries. We talk about basic security and best practices. We will show you a small demonstration and practical examples about some tools you already know perhaps or not. We talk about an open-source toolbox for industries, and at the end of this session, I hope we will have some discussion, some questions and answers, to share experience, to share what you are doing about security and maybe

what you are expecting from TLD Ops. We have just the steering committee session before and we are working on the next-year roadmap for the group. So we have ideas, but if you have ideas of what we can do to help the community of the ccNSO working on security aspects, please share with us and we will be pleased to have your feedback, okay? Okay. So, the essential role of registries in the stability of the Internet. You know that we are working for registries. We are having a fundamental role in maintaining the stability and reality of the global Internet. We are the ccTLDs. And we are entities responsible for managing domain name [inaudible] and ensuring that DNS is working. So that may explain that we are here to ensure that we have continuity of access, trust of digital identities, technical resilience. I think it's clear for all of you, but it's important always to remember that. And we have to ensure these kinds of things. Registries are high value, high-impact targets because we are [underpinned by internal stress and operational] stability. Attacks on them can have global effects that can have economic effects, marketing effects. Critical services cannot be reached. So it's very important for us to be resilient. And we know that we are working on the DR/BCP. We are working on DDoS attacks. We have made some deliveries to help ccTLDs to face with these kind of attacks. And we've got security issues every day. We are potentially the aim of cyber attackers now. Even if DNS resolution is not the most attacked in the world, because we see everyday attacks to companies, defacing of websites and things like that, it's very important to say that it's one of the priorities of the tech guys to ensure that security and that the DNS service is

working. And we are targets. We are targets. Why are we targets? Because of few things. So first of all, we are critical national infrastructures. ccTLDs are considered part of the nation critical information infrastructures. And if we are compromised, we have major national consequences, including the shutdown of government websites—for example, online services, digital communication platforms. For example, in my case, I'm the CTO of AFNIC, the.fr registry. If we are attacked, I think about the resolution. Most of the government sites won't work anymore. Public communications will have problems, as well as national commerce, banking, media operation and so on. After that, we have got national visibility and reputation. We are visible entities internationally. So a successful attack against one of them, one of registries, [will be paid attention to] and can severely damage a country's digital reputation. So we have to work together to face these attacks, and it's one of the aim of the TLD Ops group to share information and to share attacks when we are the aim of these attacks. And it's important to fight globally and fight, all of us, against these kinds of things. Of course, they are high-impact in the event of compromise. Millions of domains can simultaneously be damaged. So we will define more precisely this kind of thing with the traits and the best practices, but we all know that we are very important structures in the country. We are also vectors of trust and geopolitical leverage, and the viability in the level of protection is important also. That's why we must raise our level of security every year—every day, I say. In Europe, for example, we raise our level of security with the NIS2 directive. We have to raise our level

of security. I know that in other parts of the world, the level of security is raising also. So it's important to us to know that we are targets like the others. So, that was just an introduction to that, but now let's dive into some illustrative examples of attacks. Guillermo, if you want to start.

GUILLERMO LAMA

So we last year—I'm Guillermo Lama from.cl—we faced an incident. At the beginning, we never noticed that it was an attack because nobody had seen malfunction on our systems. There was no apparent disruption of services. It was stolen credentials used on our registrar to modify the domain DNS primary servers. We never reached the real attack that we had, but we noticed about 100 domains compromised. And we began to enforce on all parts of our security because everything was mainly focused on our network cybersecurity, not on business logic or procedure. So it was a large review of cybersecurity. And in the last year we reviewed every business process in our organization, including non-technical issues. That means, until the last year, we had divided our experience into technical and non-technical. Now we discovered very painfully that everything is bounded and must be reviewed as an entire system with technical issues, procedures, and awareness for the whole organization. So I don't give you more examples from the technical side because It's very interesting for technical guys, but in this example I want to show you, security from the registry

operators can be compromised in a way that has been seen on our farms. Thanks, Regis.

REGIS MASSE Thank you, Guillermo. I will share with you another example that took place in France last year. Okay, today we are about registries and security for registries, but don't forget to have some security for registrars too. Last year in France, one registrar had an attack, a [non-similar] attack, followed by a DNS incident. Okay, we can say, "Okay, it's a registrar; it's not as the registry," but when a registrar had an attack, there were a lot of domain equation for.fr, and DNS abuse for.fr [was] raised after this attack. So the registrar has announced that it has been the victim of this cyberattack two days after the attack, and the company says "We have been victim of a cyber security, "mobilizing in teams and crisis units, of course. But we have the role to help them to stop the attack on the registry side. Two days later, it provided further information about the incident on the same channel. And it said it was a ransomware attack. Certain services (hosting an API, for example) were available. And they asked for the registry to help them, the CERT in France, cybersecurity experts, and for a lot of people to raise this crisis. This example is just to imagine that we are in an ecosystem. We are not alone as a registry. So if the ecosystem is attacked, the registry can have effects on this attack. It is important also to be aware of that and to help the registrars raising their security. We will see, during the [break] practice chapter, how we can do that For us, for.fr, for example, we are making a lot of things with the registrars to raise

our security; so their security, so our security also. And it's not always easy to find where is the problem, where is the issue. What is important also is that we see that for the last 10 years with TLD Ops, it's more easy to speak about an incident, but it's difficult to speak about security issues. And one of the main goals of this group after sharing contact is maybe asking for help, and we're working with trust contact. We know a lot of each other. So it's important to share things that can be shared, of course. So, trade landscape for registries, Guillermo. You've got the floor.

GUILLERMO LAMA Thank you. Please, next. What we've seen since from the beginning are many common attacks to ccTLDs, but now we can resume it in some areas that must be attended and need observation. So first is the large-scale phishing campaigns via ccTLDs. They're using not only dot-coms or gTLDs; they're using ccTLDs for any reason that are used to trap users, as in social engineering attacks, to steal information or misuse their accounts. So observing these threats is very important. I don't want to do advertising for any company, but NetBeacon is one actor that is publishing and consolidating phishing attacks reports. You can receive it and it's very useful. Bounded to it, it's the abuse of ccTLDs for spam and malware hosting. Usually we used to see if the name was working or not without any concern about the content that was published under this name that was registered. So taking a look at the content that is used or mailed using our domains must be an important issue by now. Well known are DDoS attacks against this ccTLD

infrastructure. Anycast clouds and networks are useful to prevent them. If you have resources … At least we in Latin America, we have several options that are sponsored by our regional organization, LACTLD, to help us to prevent and mitigate the DDoS attacks. And for me, the main issue is the evolving attack strategies and technical innovation. It's not the newest issue that we faced. But many botnets are using automatic generated domain names to use these command-and-control botnets. We must be aware as ccTLDs that our domains are not misused for these command-and-control botnets. So one part of our motivation is to recognize them (maybe not to hunt because it depends on the local regulation) for how you will act. But a ccTLD should be one of the first alerts that some domain is misused for these purposes. Next. So specific challenges for risks and risks for ccTLD data registries is high volume and a heterogeneity of zones. That means some registry administrators must handle with a lot of registries or zones that make difficult this monitoring and awareness of what's happening. For sure, limited resources and response capacity, I think, is one of the biggest issues. We are not used to having a big security infrastructure like [CERT] that are supporting the majority of the TLDs. We sent a survey. I want to ask you here in the room. If somebody answered the survey that we sent, please raise the hand. Or nobody? One. You don't know? Yeah, that's an answer. And that's one of our problems. We are not sure if this poor answer is from a lack of resources of our ccTLDs or another problem that we might discover during this week. So limited resources and response capacity is one

of these issues. Another point that is handled in many ccTLDs in different ways is divergent or weak registration policies. Please.

KRISTIAN ORMEN: Just a quick question. Kristian from .se. Is there a way to see if we answer these? Because normally we would answer all these kinds of surveys. So if we didn't, we would want to [follow up].

GUILLERMO LAMA: Sorry. I can't remember your name and where you are from.

KRISTIAN ORMEN: Kristian Ormen from .se.

GUILLERMO LAMA: Thank you. I will check you, and in this session we can check it.

UNIDENTIFIED MALE: Another question.

GUILLERMO LAMA: Please.

ABDALMONEM GALILA: Thank you. Actually yesterday we were discussing the worker group of disaster recovery, and we were discussing the topic of crisis. I think one of the crises is the lack of disaster recovery sites

that should be added here. Maybe, as a ccTLD, I am not aware about what disaster recovery is, what does it mean, what is important for. And this could be one of the crises that should be considered for these challenges.

GUILLERMO LAMA: In previous TLD Ops sessions made in the past years, there has been written a DR/BCP playbook that is useful for ccTLDs to implement them on their own business. We will review if it's published or not, and maybe that answers your question because it must be implemented on their own ccTLDs. There is no general policy that coordinates every ccTLD to respond to disasters. It must be handled by every ccTLD on their own.

ABDALMONEM GALILA: Yeah, you are totally right. But actually there are some crises that are out of your hand. Maybe it's a flood, maybe it's a war, maybe other things that will happen on the fly away from [power cut or condition cut]. So one of the changes is that I will not have disaster recovery on the cloud in other areas other than my country in order to have this data again and online again or somehow data is [corrupt] for my registry data.

GUILLERMO LAMA: It's a very good question. I don't want to … Maybe we can talk in a few minutes at the end of session, but what I can tell you is, when you talk about that we can't handle some crises, part of this

DR/BCP procedures is to recognize if you can or cannot handle some type of crisis and what you will do with this instance. So a common example is we have a service provider. It's a cloud provider. We lose connection to them and we make him responsible for our data. That's not the right point of view. The right point of view is, if I lose something, how can I recover my systems with this lost status? It's: when your wallet has been stolen, you must see how to get your credit cards again. You can blame only the thief because you don't have your wallet. So you can be tempted by them, especially if you're bounded to providers that you have a good relationship with. Or, like in my country, we used to have earthquakes. But the modern approach to this [theme] is being prepared to face this incident and survive them and for sure have a disaster recovery plan that enables you the operation continuity.

REGIS MASSE

Just one point. We were talking about that yesterday during the session to prepare the Wednesday session of the session. So during my presentation next Wednesday, I will try to just present a landscape of crises. There are seven groups of crises that we have described in the DR/BCP playbook already. And I will be happy to exchange with you if you have some other ideas about that. Yes, Alejandra?

ALEJANDRA REYNOSO

Thank you, Regis. This is Alejandra Reynoso from ccNSO Council. Just to address your point on getting more responses to your survey, maybe an idea would be to talk to the Tech Day leadership, in case you can put up on screen a QR code for the members who are present in the room. That tends to be a very full room of CC tech people. So that could help you get your numbers up. And this idea comes from the IANA survey; the responsible people. They were also looking for more responses. And they started even handing out cards with QR codes for the survey. And that would prove to be very effective. So just an idea for you to get your numbers up.

REGIS MASSE

Thank you for this point. Yeah, thank you. Sorry, your name and your question, please.

BARRACK OTIENO

Thank you very much. My name is Barrack from AFTLD for the record. I just wanted to add the aspect of social engineering. We are noticing … I'll speak of Kenya specifically, where, for instance, someone approaches you in a meeting like this, and they have a valid domain name from a ccTLD representing, say, ICANN—only that it has three Ns as opposed to one. And they probably know that there's a constituency behind you or you're a community leader and they say, “We are looking for this kind of expertise. Would you reach out to your constituency and see where we can find it?” And once you provide the email address, then they start scamming the group. They say, “Okay we need a certain set of documents. We can

help you to prepare these documents, and you need to pay X amount of money." So it's a very subtle way of scamming in which trust is involved. It's a trusted network of individuals, but I've seen it happen twice in Kenya involving community leaders. And maybe it's something that we need to be on the lookout for. So it's no longer the straightforward scamming, but they use the credibility of structures in a community to perpetrate scams.

GUILLERMO LAMA So if you go a few slides further in our presentation, at least you will see there are tools and things for information sharing that I think is the point to make aware the rest of the community if we are being threatened by some attacker, hacker or whatever name you want to give to them. But the point is, as I was explaining, first, the challenges that we have is complex multi-stakeholder collaboration. It's an explanation you asked of specifically. It's a challenge to have an orchestration that enables the ccTLDs to respond not only to threats that are directly attacking your ccTLD. Maybe you're only the vector to attack our staff, and that's part of the view that's cyber security companies are viewing on our landscape. And the other specific challenge is that every ccTLD has different attribution and investigation difficulties. Not every ccTLD has the same tools, the same procedures, so to standardize our efforts will depend on how similar our behavior from other ccTLDs is. So in summary, I could say this is a complex scenario. It's hard and difficult for us to enable some very generic tools or very generic procedures. So we must be aware of at least these points and then

see which tool can be used or which procedure can be implemented. Thank you, Regis.

REGIS MASSE: So we will try now to speak about basic security best practices. And the floor to Angela.

ANGELA MATLAPENG: Hi, everyone. My name is Angela Matlapeng from the Botswana CSEd, which is also the .BW registry. So I guess you've heard about some of the incidents and challenges that ccTLDs are faced with in terms of abuse. And this morning we will just look at some of the best practices that could help mitigate some of those incidents or even prevent them from occurring. So next slide, please. I think I'm going to ride on what's been said with social engineering, the goal of which is always to get access into systems. So with securing administrative access, the objective really here is to prevent cyber attackers from getting access to your registry portals, your databases, and all the important systems that are part of the ecosystem. So if there's a compromise really at any level that could allow these attackers in, you could get your traffic being redirected to where you don't want it to go. There could be entries into the systems themselves which compromises the integrity of the information that's being held by the registry. So some of the best practices we're looking into is enforcing multi-factor authentication, which means you've got another layer of security in addition to your username and password to authenticate that

it's really you. So this could be, for instance, a one-time PIN that's sent to your text number. It could be a digit that you get from your own authentication app, maybe like Google Auth or Microsoft Auth and stuff like that. So that's just one layer to that. And oftentimes we find that not a lot of registry users would have this in place. And once your information is out there, which in our instance we've got access to [paste beans] and all that information that's available freely on the dark web where anyone can get access and try to get into your system. So this is one way of restricting that. You've got the principle of list privilege. So it's just to say that whoever needs access to certain roles should only be allowed access to those roles. So it's not say everyone has got general access to all the systems. So it's just restricting account privileges like that. Example of tools that you could use listed here is Keycloak. So for your identity and access management, that's an open-source tool that you can use. We've got, for your zero-trust authentication, Authelia as an example of a tool; Teleport if you want to secure your SSH sessions. All right, so now we speak about hardening the infrastructure itself. And really the objective here is to prevent tampering, redirection of traffic, interception of communication, and any activity really that could undermine the trust in the domain space. This would involve cryptographic protection and clean configurations or good configuration practices, right? Solutions that we could implement here include having DNS update security. So if you've got, say, a primary server and a secondary server, and you need to transfer zones from one to the other, you should have ideally security to prevent interception or even if that would happen, there should at

least be security to make sure that no one is tampering with your zone transfers. So tools that are being suggested here is your TSIG for zone transfer and OpenDNSSEC, on which I think I should just mention that NLnet Labs has since announced that between October now and October 2027, there's going to be an end of life for OpenDNSSEC. So they're introducing Cascade, which they hope to release the production of around 2026. So there are alternative tools that you could use such as Knot for this kind of security. Alright, so another area to look into is infrastructure monitoring and zone monitoring. With this, we're really aiming to harden configurations and monitor any transactions between name servers, for instance. So with domain configurations, Zonemasters are a good tool that could help you test whether configurations have been done properly, and you also have infrastructure and availability monitoring tools such as Nagios and Zabbix that's been listed here. Wazuh is another security incident monitoring tool that you could use to help out with this session as well. Okay, hold on. All right, there we go. Someone spoke about backups and incident preparedness. I think most of the sessions that we've had spoke to this aspect with playbooks and all that. And really this part of preparedness is just to help you be able to detect and respond to incidents as and when they happen and be able to recover within stated SLAs and continue with the register operations. So key practices here is just to have your playbooks and make sure that you run the playbooks. So this would state actionable procedures for incidents such as your DNS tampering if that was to happen. Phishing has been a very a common example that's been used here;

denial of service and natural disasters as has been mentioned in the room this morning. You also need to be able to detect and triage in action all incidents that you get with clear communication paths to say, okay, if there's an incident happening, who has to take charge and control of all that? What are the clear roles that are being stipulated there? Because guess what? You can have all the tools to help you do that, but if communication is really not clear, it could delay the response itself. You should be able to capture evidence and forensics. I think one of the challenges that we have with incident detection is the inability to attribute, to say "this is where this is coming from" and all that. So being able to automate? With the rise of AI tools, you're able to do that. You've got your WHOIS information that could also give you an idea if there's anything wrong going on. So you also have the registration of new certificates, for instance, if the domains are being registered with malicious intent. So you should be able to capture this evidence and if you do need to file takedowns and all that, you should have those templates ready to help out with that. Communication and legal: these are some of the functions that could be outsourced or for some registries, they are in-house. And going back to clear communication, we need those templates that are already approved according to the standard of your organization and having legal in mind, especially if you're dealing with takedowns, because it could be a little tricky if not everything is taken into consideration, particularly where a domain name is involved. And we know if it's taken down and it's not really malicious, it could have legal implications. And of course, exercising these tabletop

drills just helps with improving the process itself. And there's regularly checking if you've got the right visibility into your incidents, if you've got the right tools to help you with incidents that you're faced with as a registry. And also, I guess, is just ironing out the communication part itself, being able to figure out what your priorities are in in terms of how you respond when there's an incident and who's got what responsibility and just figuring out coordination. Post-incident review, which is lesson learned, updating your playbooks, and all that for future improvement is very important. So I will pause here to give to the next speaker. But if there's a question or comment …

NATHAN MEURRENS Hello everyone. I'll give a few words about anti-abuse practice. Anti-abuse is actually a bit of a side topic when it comes to security for a registry, because actually domain name abuse and especially registration abuse is not a direct threat to our operation and our business continuity as a ccTLD. You might even consider sometimes the opposite. So is the microphone a bit... Or am I talking a bit too loudly? You might consider even the opposite. I mean, if you don't mitigate abuse, you will probably have more registration. Yet, of course, it has a very big impact on our reputation and on the security of the Internet in general. I mean, we had an example earlier about this ICANN with three n's domain. Yeah, of course, you don't want this ICANN with three N's domain being registered under your TLD. So from that perspective, we have to put in place anti-abuse measures and abuse prevention

measures. Actually, I would be curious to know in the room here, in the audience, how many of you do use some specific tools to manage to prevent abuse or to react to abuse? Okay, so apparently we are not so much. Well, the good thing is there are tools that are available for this. Databases. Probably Spamhaus, Yeti—some database that are available providing information about abuse in domain name registration. And there are even tools. I think tomorrow during the … I mean, we use [inaudible][eu]. We use an abuse prevention system pre-delegation, AI-based, to detect malicious abuse. We even have a free version of this available if anyone is interested to test it available as a SaaS. I think it will be presented tomorrow during Tech Day by some colleagues. So there are solutions that you can put in place like indeed AI-based solutions that are growing now and databases that are existing, and the malware information sharing platform, MISP. So all of this you can use pre-delegation or post-delegation. The idea is indeed to detect ideally pre-delegation but even post-delegation at least to detect any abuse before it is reported by the authorities. So that's what I had to say about abuse for today.

REGIS MASSE Thank you, Nathan. Okay. So, it's the live demo's part now. I have chosen to show you some tools. Maybe, as I said, you already know them. I have taken four topics about security, just something about DNSSEC, something to analyze the DNS zone with Zonemaster, talking about SPF, DKIM and DMARC and RIPE ATLAS and DNSMON. Are people in the room that already use this kind of things? If you

can raise your hand. Yeah, I saw him. Okay, so it's just to show some examples of free tools used by the community of the DNS to analyze things and, when there is an issue, a security issue, to try to understand why there is this issue. So I will try to share my screen. This one. I will take this one … Okay. Poof. First of all, okay, first of all, you've gotten a tool for DNSSEC that is called DNSViz. This is a tool which makes some analysis of your DNSSEC configuration. And it shows easily where are the problems. So I have [two to] fight against no one. I have taken my zone, afnic.fr, and say, for this moment, everything is green. So we can see the DNSKEY, the records in the DNS to define the keys of DNSSEC, and you've got the chain of keys in all the section. But sometimes there are problems. It's difficult if I don't see my tabs under that. Okay. I will try to do that. Okay. This one. The DNSViz is recording all the things you have done and all the requests that was created on the DNSViz, on the system. And I found.au. I found this one. It was an example, but there are many others. We saw that in '24, on the 30th of January, there was an issue with DNSSEC. So you see it easily. There are red lines. There are yellow lines. And they tried to explain what are the problems. And you've got the problems here, visually, to say that there was a problem with the DNSKEY and other parameters. I try not to be too technical, but there were problems between these zones. And 13 errors. And these tools are very easy tools to use for registries and can easily show you where are your DNSSEC configuration problems if there are any. Okay, so DNSViz.net. And if you got there, you are just to enter your domain name. You can use what we want. If I launch here, I can update now [and] analyze

the system; so analyze in real-time what happened, how the zone is configured. And then you can see easily for … Okay, I don't have to call my team. Everything is fine for dot.fr and AFNIC.fr. A second example is Zonemaster. Zonemaster is a tool developed by .se and.fr. I prefer to say .[fe] because it's hard for me to say Internet [Stifelstone.] Sorry for that. So [inaudible]. But it's a collaborative project that we are doing for a long time now. And the goal for this project is to analyze a zone, analyze a DNS zone. And to aim at no ccTLD this morning, I've just taken this example, for example: icann.org, So sorry John for that. But the good thing is there is only one warning, so for ICANN everything is good. You can easily analyze the system, the basics of DNS and for example, connectivity. I will see that there is a warning here. I will check it and I say, oh, okay, the DNS.ICANN.org does not respond to query over TCP. Okay, DNS is over UDP usually. We try to use it with TCP and I've got this warning this morning. So it's nothing. It's not very important, even if today, we will see with the Atlas probes, there are a lot of requests with TCP. So it could be something to involve. So this tool is free. The good thing for this tool is, okay, you've got the SAS version, but you can get the source, implement in your registry and use it in your infrastructures. Yeah, the source is free. It's open-source. So you can use it and deploy it in your infrastructures easily. So for example, sometimes we've got things with DNSSEC. There is no problem here about name servers. We can get the version. Okay, it's just an information, but this tool is … It's not my team that developed on that. It's the R&D labs, R&D team, of AFNIC. So I can say that we've with the Swedish guys are

doing they are doing a very good job Third examples about SPF/DKIM/DMARC. It's a good thing today to consider that emails are a way of attack. We have talked about DNS abuse, but mailing, emails are very used to attack things with phishing, with a lot of attacks and things like that. And we've got today free DNS records and a free way of fighting email attacks with DNS. It's SPF, DKIM and DMARC. SPF, just to remember, is to verify that the sending email server is authorized. DKIM is to manage integrity with certificates. And DMARC is to define policy action if SPF and DKIM fail. So with policy action, you can send reports to the owner of the domain name, and also you can say, okay, I want to reject this email, I want to put in quarantine or I want to accept it. And we have, for example, at AFNIC, studies, since three years now to see how SPF, DKIM, and DMARC are involved in France from French government. And for those who will be at Tech Day (small advertising). For those who will be at Tech Day tomorrow, we have a presentation with Benoit, my colleague, about SPF, DKIM, and DMARC, and the way we can use it and the observatory of.fr. But as I have the permission of the CEO of .bzh in the room, I can say also that we have an experimentation for.bzh. It's a gTLD. Sorry about that, but there is something just … where is it? Where is it? Where is it? No, this one. I have to find the good tab. Oh, I don't know. Okay. So we have an experimentation in France for .bzh to implement, since the beginning of September, DMARC. And we have just an implementation of a small dashboard. Sorry, it's some parts. Oh, okay, yes. Ah, okay, you don't see the good screen for … Sorry. Okay. In this one … yeah, sorry, sorry for that. I don't know.

Okay, so this dashboard is a very small dashboard. It's an open-source tool. You can get it on GitHub. And it's just to see how we can exploit the reports, because reports for DMARC are JSON files. It's not very human-readable easily. And in these things, okay, reports are coming. You can have … Sorry, it's taking a long time, a bit of time, because it's just a small experimentation for us. If I take this domain name, you see that someone has tried to send this email, and here you've got a report. Just importantly, .bzh and AFNIC are working with [the set of Brittany]. I will talk about that. And they are trying to develop a platform to analyze DMARC reports, and they want to make it open in open-source. So maybe you will have access to these kinds of tools in near future to analyze DMARC and DMARC reports. And I will talk longer about this experimentation tomorrow. And the last example I can give to you today … Okay, okay. Stop that. It's about ATLAS probes. Do you know already ATLAS probes in the room? Yep, some of them, some of you. Okay, so there are two ways of using DNSMON with ATAS probes. You can use the DNSMON … I'm sorry about that. I've got the Zoom bar just in front of my tab, so it's a bit difficult. DNSMON. Okay. When you use DNSMON, the opens version, the free version, you've got a way to see if your zone … There are a lot of TLD zones in present here, and you can see if there are troubles with the data probe system. Just to remember, ATLAS probes are a lot of probes deployed all over the world. You can have them yourselves, you can have them in your home, in your infrastructures at your company, and they make measurements of DNS, of websites, of a lot of things. And for DNS, you can see easily if … For .fr, for example, I

can set a resolution for 5%. Okay, the resolution since yesterday is okay. And you can have details. For example, I take one error. DNS cloud. We can see, okay, these are the probes which analyze the things. And you see sometimes, for example, there is a probe in the United States who have trouble to query [sense], and there's no query for this probe. So it's just to see something. It's not to analyze very clearly what's happened, but DNS probes behind that[.] You've got APIs, and you can use the APIs to get the information and analyze information. And what is interesting with ATLAS probes made by RIPE NCC is, if you've got your probe, you have credits. Giving the information to the community, they gave you back credits. And with the credits, you can menu all measurements. And I have just made one this morning to just show you easily a demo. I have just made a small measurement to try to ping the AFNIC website. It's just that, and I have taken 50 probes all over the world. You've got the map of the probes. And you can have the time in which the probe gets the response from the website. Okay, so you can do it on DNS, on websites. You can have measurement on a lot of things. And I see that 49 probes reach their targets. So if I wanted to analyze, I have to analyze further the measurement to see what happened. But with the credits, you can make your own measurements, and you can use also the API ATLAS probes to make some specific tests, make some specific measurements, trying to find and analyze what happens to your DNS zone or to your name server or to a website and things like that. Okay? So there were just a few examples. I think a lot of your tech guys knows already these tools, but in a way to share things

with the community, it's important to say that there are a lot of tools free to use, and you don't have to pay a lot of money to use tools to analyze things on the internet. You can. That's all. And we will now show some example of tools that your team, the IT teams, can use to analyze and to fight against cyber security. If you can take me back to the slides please. Okay, we're back. And now I will give the floor to Josh.

JOSH SIMPSON Hello, everyone. I am Josh Simpson from InternetNZ, the ccTLD for New Zealand. So let's have a look if we can get there. Right, so we're just going to cover some key open-source toolings that your operations or technical teams can implement in a couple of different areas here. So one of the things to start out with, which we haven't covered too much yet, is monitoring and alerting. I mean, you can't really manage what you're not measuring regularly and the availability of the services that you're providing as well as the integrity and what is actually happening with those. So there's a number of open-source tools that can assist you with that. Nagios and Zabbix are some well-known ones for monitoring your infrastructure. They use the concept of generally remote agents to install on individual systems to monitor things like processes, availability of services, whether they be operating correctly or incorrectly, returning responses. Generally, what you want to know you can configure them to check for you on a regular scheduled basis. Another tool option in that regard is Prometheus, which is sort of one of the newer entrants into that market. I mean,

it's just been around for a while, but that's more of what's known as a time series database. So you actually have your measurements scraped into Prometheus on a regular interval, allowing you to do more in terms of trend analysis and things like that. So it's useful for integer-based metrics like uptime or availability, system load, things like that, as well as response times, and can be configured with lots of project-developed tools called exporters that can monitor specific things. And there's also a lot of community efforts to develop those as well, including ones related to DNS availability querying, and the like. There's also another application that goes with the Prometheus called Alertmanager which allows you to obviously run rules against those time series and that can then alert you to issues on thresholds that may be of interest to you. So for example, if your server's been compromised and there's crypto mining or something like that, you can monitor the load and alert on high levels of load on your server when that should not be a common thing that's happening. And moving on to the DNS analysis and security, as we just demoed earlier, we saw the graphical interfaces of Zonemaster and DNSviz, but those are actually public services. In addition to those, you can run the actual tooling on premise internally on your own infrastructure to test more frequently and have that internal viewpoint. And that's more just trying to maintain best practices with zone quality. Zonemaster provides test cases, a test engine, a command line interface, as well as the server and the GUI that was presented. So that can be self-hosted as well. DNSViz as well can also be self-hosted. That is also a command line tooling as well as it can output

many different formats, such as the images and web pages that you saw, but also you can output things like JSON and other things which you can integrate into your alerting system. So you can schedule internal analysis of your zones on a regular basis and alert on those, for example. Another option here that can help is DSC, which is the DNS statistics collector. That's a two-part tool that's developed by the DNS-OARC group. And that's a piece of software that runs on your DNS server, capturing all the DNS packets and producing statistical analysis of what is actually coming in and out of your server. And from that there's a presenter analysis part that can allow you to visualize those patterns in your DNS traffic, for example, so you can pick up on bursts of traffic. It'll tell you what types of protocols are being queried, whether it's UDP, TCP, and a lot of other useful information that's presented in a graphical format that can let you see what the normal state is but also delve deeper into problems that may occur. Another tool is an identity and access management was mentioned earlier, which was Keycloak. And you can think of this along the lines of a self-hosted SSO or single sign-on solution. And it can integrate with a bunch of other components in your internal system that can allow you to centralize your authentication, supporting standard open protocols like OpenID Connect and OAuth 2.0. So you can integrate all of your internal tooling as well as potentially some externally facing tooling depending on how you present services to your customers that allow you to centralize and enable modern web practices with regards to authentication, which can be really useful, whether that's TOTP rolling codes or passkeys. It allows you

to do all that without having to delve deep into the implementation of those specifically and integrating with the tool. Also mentioned was cyber threat analysis or MISP. So there is a project called the MISP Project which is an open-source threat intelligence platform, and that allows you to collaboratively share with others on an agreement basis in terms of the threat information, and that's based on indicators of compromise within a community of trust. So it enables you to store, correlate and distribute intelligence internally and with external partners that you agree with. And an example of that is consuming external threat feeds, whether they be from your local CERTs or other players in your domestic market or international market as well. An example of that is the AbuseHQ parent company, Abusix. They produce a global reporting project for free abuse reporting in an open transport independent language that you can integrate tooling like that. And we'll get to the next slide. There we go. So other options on more advanced side of things you can consider is security information and event management. So that's where you're centralizing all your logs and other information from all of the systems that you operate to have more of a correlated view instead of a siloed view of things that are happening in your infrastructure and environment. And yeah, it grants you the ability to identify threats happening across or moving throughout your infrastructure, for example. And that can be from your servers, from network elements, firewalls, endpoints, including not just on the infrastructure side but on the operator sides at laptops and operators interacting with your systems. And that can trigger real-time alerts and the like if configured to do so.

Other tooling is vulnerability scanning. So you can do vulnerability scanning yourself in addition to having third parties do it, and some of the tools there, OpenVAS and Nessus, allow you to deploy these types of things within your infrastructure to be proactive with regards to what's running on your systems, if there is stuff that you don't know about, as well as (so there's a method of discovery there) to assess stuff that you actually do know about, and is it running an up-to-date patch version, for example. Another thing that was mentioned earlier was sort of DR[,] and other things and automation and orchestration of your configuration and servers and other IT assets with regards to your operation can assist with that. So this is moving into things where you're talking about infrastructure as code so you can rapidly redeploy your services in the event of an issue, and some of the tooling for that is mentioned here is something like Ansible or SaltStack. So SaltStack is an example of an agent-based where you have an agent on each system, and Ansible is an agentless option, so it's deployed over an SSH push configuration. And that allows you to achieve a repeatable deployment. So when you make a change, you don't make a change on the system; you make a change in your automation. And then your orchestration pushes that change out. And it's a repeatable and the same across multiple systems of the same type, for example. And finally, we have incident collaboration. So DFIR and IRIS and Matrix or Mattermost are examples of sort of internal communication. So if you do have an incident, it's being able to communicate securely with other members of the incident response that you are set up and working

with. So Mattermost is a centralized piece of software for internal communication between teams, and Matrix is an example of a decentralized one where you have no central point which can be useful in some situations. And with that, I will pass back to Regis.

REGIS MASSE Thank you, Josh, for that. To end this session, some interaction with you. I think we will not be using the Mentimeter. We are not very ready for that for the moment for the group, but you can raise your hand for your registry experience, DNS attacks, phishing campaign, or data breach, if you want to share something about that. Wow, lucky you are. Lucky you, I have no one. Ah, yes, I saw one.

JACOB ZACK Hello, Jacob Zach from CIRA, .ca operator. So we are frequently targets of DNS attacks, DDoS generally, given that we operate Anycast for a large number of top-level domains currently. And tools that I would mention here would be things along the lines of NetFlow, something like Kentik or other tools like that, that immediately give you a view of where traffic is coming from, nations, networks, types of protocols, flags in those protocols, etc., to help you identify patterns and then IP tables or ACLs that allow you to block that traffic. I also mentioned that in a lot of cases, slides that I would recommend for this particular workshop would be perhaps like a community slide. I know that a lot of coordination is done within groups like TLD Ops, but as well as DNS-OARC or

other things along those lines, where you can find others that have experienced or currently are experiencing that same attack and coordinate efforts to cease those effects. Thank you.

REGIS MASSE: Okay, thank you. Another comment. So the three questions are very close, but [it's] the type of incidents and the most effective countermeasure you have. If you have something to share. If you don't, we can just go to a discussion if you want to share something, if you want to ask, if you have questions. Did you find this session interesting? Yes, Barrack?

BARRACK OTIENO: Thank you, Regis. Yeah, it was very interesting. I've taken a lot of notes here. But having said that, one thing that has not come out very clearly for me is that a lot of the attacks are aimed at the reputation of organizations. So probably [have] a slide outside the technical remit on steps that an entity could take to safeguard its reputation because you realize you may have a lot of these tools in place, but you may have a very small window to actually explain that everything is under control. So maybe it's something in addition to that regard.

GUILLERMO LAMA: So your remark is very interesting because one of the points we were looking for with the survey was to hear possible reputational attacks that we have directly or not directly to the ccTLDs. But as I

	said at the beginning, it's not a standardized attack. It depends on your region, your culture, on many facts that we want to collect. And we hope Alejandra can help us to publish our new survey on Tech Day maybe.
ALEJANDRA REYNSOSO	Sorry, can you repeat again?
GUILLERMO LAMA	Don't worry, you mentioned before that maybe you can help us to publish, with a QR code or something similar, our survey or a new survey that we want to send. So we count on you with your help. I appreciate help.
ALEJANDRA REYNOSO	Okay, if you give me the link, I can put you in touch with the Tech Day leadership.
GUILLERMO LAMA	Thank you, Alejandra.
REGIS MASSE	Is there other questions on the Zoom? I just look at the people. Yeah? Oh, yeah, sorry.

ADITYA VIKRAM DUBE: Hi, this is Aditya Vikram Dube from India. A couple of observations. Really great presentation and quite thought-provoking. First of all, on the issue of jurisdictional challenges, that is something that is quite important from the context of DNS abuse emanating from a different jurisdiction and a court order being initiated in that jurisdiction and its enforcement in a different jurisdiction, and that gets blocked maybe because of different privacy laws or consumer protection laws and stuff like that. So some sort of commonality or agreement between different countries on addressing these jurisdiction challenges is something that I think ccTLDs can work together on. And the second thing is also about from the context, not specifically from the ccTLDs perspective, but more on those ccTLDs which also run national Internet registries perhaps. So, you touched on DNSSEC and the different tools that you can use for the DNS perspective, but also from the routing layer, perhaps the BGP layer and ROA and ROVs and its implementation by the national Internet registries to sort of address that. That is also important, perhaps not from the entire ccTLDs' perspective but from the NIR's perspective, I guess. Thank you.

REGIS MASSE: Other questions? Remarks? Yes, Barrack?

BARRACK OTIENO: Thank you, Regis. Just a comment. I noticed that the presentation is largely focused on the registry and registrar who basically run the infrastructure. But I was trying to think of where we can bring in a

registrant. One of the other things that I do back at home is a lot of cyber hygiene awareness for the public. In our country, Kenya, we have a government program targeting 20 million citizens by 2030. And I've been walking around with some cards I got in the disaster recovery play session we had, I think, a couple of sessions ago, and I was just wondering how can we turn this into some sort of game or something for the normal masses because that's now the weak point or one of the vectors that we have to deal with. I know we may not have the answers in the room, but maybe it's something that ICANN could consider through the grant program to come up with a game or something that targets the end users.

REGIS MASSE Thank you, Barrack, for your question. Yes, that's true. The goal, the main aim, of this presentation is for registries because TLD Ops is the collaboration of registries—and ccTLDs especially. But yes, I think we have to promote security on registrants now, not only registrants or registries. And yeah, I don't have the answer yet, but I think it's something to think about, yeah. So I think we are nearly run out of time. Just remember that you've got for ccTLDs, key cooperation channels, you've got TLD Ops, us, you've got IANA, you've got the European TLD, and I know there are other ISOCs in the world. Of course, all your regional forums, APTLD, AFTLD, CENTR, ccNSO, [inaudible] ALAC TLD. You've got IETF, you've got DNS-OARC. And yes, that's [why those are] your points. I understand that there's a lot of communities, a lot of groups, and the difficulties for the moment is some time to call to make every

group work with each other. People are going to IETF, people are going to DNS-OARC, I'm going to ICANN. So sometime, yes, if we could find a way to work together better and better on that, it would be interesting. So I want to thank you for joining us this morning. I hope this session was interesting, and I will tell you, I will wish you a good ICANN week. It's just the beginning. And for technical stuff, there is Tech Day tomorrow. And after that, during the ccNSO, I think we will have some discussion. And all the [TLD] group [is good], and I want to thank them for making this workshop successful this morning. Thank you, all. Yeah, we are here to share with you about security and about DNS and about all the things and about what you could expect from TLD Ops if you have got ideas on that. So thank you.

[END OF TRANSCRIPTION]