KELVIN WONG: Okay. Hello, everyone. Can you hear me? Okay and welcome to the APRALO APAC Hub Capacity Building Webinar. It is 5 minutes past 1:00 PM so start. This is Kelvin Wong from the ICANN APAC Hub, me and my colleagues from the APAC Hub and also from At-Large staff supporting this.

Just to give you a bit of background, the webinar series is initiated under the APRALO APAC Hub Cooperation Framework where the topics are collaboratively decided on together and we have been doing this for a while about [inaudible] and other topics have included internationalized domain names, new gTLDs, and Internet governance, for example.

So today, the topic is DNS Security and DNS Abuse, Domain Name System Security and Abuse. So if you recall last July, we had a DNS basic and DNS ecosystem webinar, as well, which is done by Steve Sheng. So in a way, this is a continuation to that webinar.

Our speakers today would be Champika and Kitisak Jirawannakool. Champika is ICANN's Regional Security and Stability and Resiliency Engagement Manager for the Asia-Pacific. He's a big part of ICANN's Global Stakeholder Engagement and SSR teams and represents ICANN in running workshops matters related to security, technical, law enforcement, and capacity building.

Kitisak is from the Information Security Agency, the Electronic Government Agency of the Ministry of Information and Communication Technology Thailand, and he has worked in Information Security for almost 15 years. His expertise is in improving the different areas such as incident response and management, Web and network security, risk management, and also [inaudible] spacing. Furthermore, he helps improve security for many government organizations and he conducts many training courses related to information security, especially IT security awareness.

I think we're in very good hands and before we start the webinar proper, I'll hand over to Ken, our new GSE intern for APAC Hub, which will run through the housekeeping rules. Over to you, Ken.

CHAMPIKA WIJAYATUNGA: Thank you, Kelvin. So a few housekeeping before we begin. If you have any questions during the webinar, please do raise them in the Q&A part at the left. The staff will note your questions and they will be answered by the presenters either in writing or during the presentation. Questions and answers will be posted on the webinar key page.

Okay. There will be a pop quiz after each segment, so do be ready to answer the questions posted in the poll part in Adobe Connect. At the end of the webinar, please remain on the call for about three minutes to answer a short five-question evaluation [inaudible] via the part in Adobe Connect. Your feedback will be essential if –

UNIDENTIFIED FEMALE: Okay. I believe Champika has lost audio and the connection, so please bear with us and let us give just one, two minutes for him to log in back. Thanks very much for your patience.

CHAMPIKA WIJAYATUNGA: And sorry for the little interruption. I suddenly lost my Adobe Connect screen, basically. Anyway, without taking much time, thanks very much for the introduction and so today's session, as we all know, it's going to be on the DNS security and DNS abuse handling. So I think Kelvin has already introduced myself and also my colleague, friend, Kitisak, as well, so we can move on here.

And then I also actually want to acknowledge Dave Piscitello, the VP Security and ICT Coordination at ICANN as well as Richard Lamb, who is also the Senior Program Manager DNSSEC at ICANN. They have contributed to these materials.

Now the agenda that we are planning to do today. Initially, we're going to discuss about threats and risks involved in DNS and later we will discuss why the security or the DNS security is important. Later, we'll spend a little bit of time on handling DNS abuse and what are the tools and techniques available, and then we will discuss some case studies and finally wrap up after discussing about the collaboration with ICANN, especially focusing the [inaudible] or security, stability, and resiliency aspects.

Now let us have a look about threats and risks in DNS. Now as [inaudible], we had another session earlier, a webinar that discussed about DNS concepts and also general understanding about DNS. Now this is kind of a continuation of that but I will try to recap the DNS resolution because this is very important for us to understand especially focusing the DNS security aspects.

Now here you can see that in the slide. There are a few components. First of all, we have the client, this could be a user device basically, that in this case, it's sort of browsing a certain domain name. In this case, it is www.example.net but in real life, you could be browsing, you could be sending an e-mail, and so on.

So here our objective is to or the client's objective is to browse this website and then download the webpage. So when the client sends the request, "Okay, I need www.example.net," basically the client is requesting for the IP address of this Web server. Now this request will go to what we call a resolver, so the resolver can be usually in a typical environment, maybe if you're at home, in a residence, it could be your ISP who provides that. If you're in a work environment, maybe your organization is providing this service. So usually, this sort of service or the server that provides this service is called a recursive server, we can call it resolver or recursive server, or a caching server. Now that server gets the request from the client and then sends the request to root servers.

As we know there are a number of root servers scattered around, so their request will go to the root server, and then the root server will give a response or a sort of reference to talk to the next level. As we all know, the DNS hierarchy, the next level is the TLD level. So in this example, the TLD level is .net. So the reference comes from the root server to go and talk to the .net main server.

And then the recursive server or the caching server will go and talk to the .net main server and ask the same questions. I need the IP address of www.example.net. And then .net name server will respond with the IP address of the next level, which is the authoritative name server, for example, .net. And then the resolver or the recursive server gets that information and goes and contacts the authoritative server related to that example.net zone and gets the relevant or the correct Web server IP address.

So the authoritative answer comes from the name server of example.net. It could be one name server, they could be having multiple name servers, as well. So once the [inaudible] the caching server gets their answer, that answer will be passed on to the client. The client gets the IP address, now the client can go and visit www.example.net or the Web server of example.net, and then download the webpage. So this is how a simple DNS query gets recalled.

So now moving on to now the next slide here. So during that process, we saw that there are a number of components that that we saw. We had a client, we had a resolver, the recursive server, we had root servers, we had other name servers like authoritative name servers and so on.

Now in this DNS ecosystem, in all these DNS name servers, there are some certain risks that we encounter. One of the common attacks are called reflection and application attacks. Now when the client send a request to these recursive servers, the recursive servers are given sort of a question to go and find, and then respond to back to the client. But in case if there is some attacker who would spoof the IP address or the identity of a certain other client and then pretend to be that client and then sends that request to the recursive server then, unfortunately, the recursive server will interrupt with [inaudible] to that client who really asked the question, it will respond to the spoof identity.

So this is where actually these sort of reflection and amplification attacks would come, so in the case of amplification attacks, the answer is quite big in size, so the bandwidth will be highly utilized. Now this can be versed actually in the form of what we call DDoS attacks or distributed denial of service or reflection and amplification.

Now here the attacker could control a number of or send a number of queries requests to number of the open recursive servers. Why I would say open recursive servers because they would or they would get the answer from any source. That's why we call open. Usually if you have a recursive server, if you have your recursive DNS server in your organization, better way to do is you accept the queries only from your client.

But there are lots of networks out there who would, or the DNS servers, these recursive name servers to accept the answer or the queries from not only from their clients but also from any other party. This is very bad. There are millions of open recursive servers out there. So the attackers, they can get use of these opportunities and then they can send these fake or spoof queries so that the answers would go to innocent parties and then DDoS-type attacks, so the resources will be fully utilized, the bandwidth will be utilized, the processing power will be utilized, and then the servers can crash. So these are some of the common threats that we have.

Cache poisoning is another DNS threat because here what happens is that, if you remember that recursive DNS server that we discussed, once it gets these answers, it saves the answers in its memory or in the cache. So when the next time when a client asks similar type of question, the same question, it can respond to that other client in a very quickly way because it doesn't now have to go and talk to root name servers or other authoritative name servers. So the answers can be very quickly.

So this is because they keep caches, they keep those answers in the memory. But unfortunately, if someone try to pollute this cache or poison this cache, then the recursive servers can answer or give wrong answers. They can behave differently and give wrong answers. So this is what we call cache poisoning. Sometimes some attacker, some miscreant can try to actually create, they can go and buy a domain name and create some domain name or a website, and then they could actually get the users, get the DNS queries, and then when the DNS servers respond, they can also actually along with those responses, they can send some other responses related to other name servers, so the caching server memory or the caching servers can keep wrong answers related to others. So these are all threats that happen in the DNS space, so cache poisoning is something that happens very commonly.

There's another common threat, which is what we call DNS hijacking or query interceptions. Usually when these DNS queries are being asked by the servers, say, if they, if the attacker hacks into a DNS server itself or it could be that to the router access point and so on.

Somehow, the objective here is that they would redirect the query into one of the DNS servers or the recursive servers controlled by them so that they can answer interrupt query being answered by the correct genuine DNS server. Now the query is being answered by the attacker. So they can always redirect you, say, for example, if you're looking for www.example.net, they could redirect you to a webpage that goes to a wrong website hosted by the attacker, basically. And sometimes it could be a financial institute website, a bank website, and so on, so you get to the wrong page and you may give your [inaudible] and so on to the wrong party.

So these are all some DNS threats that we can see in the real life. So this is also why actually we have to pay attention to the DNS security aspects. It is very important that we secure our DNS infrastructure. Now in this slide, you can see the usual components we see in a typical DNS ecosystem. Usually you would see what we call primary and secondary DNS name servers. These are what we call authoritative name servers.

So for example, if we have a domain or we have a zone called example.net, the administrators of that zone would maintain name server, a primary name server, to provide that name service for example.net and in the same way, if in case if we only have a primary name server, in case if there is some attack comes to a primary, if that goes down, then there is no redundancy. That is why we have to have another redundancy or another server or multiple name servers, what we call secondary name servers so that in case if one of these name servers are down, [inaudible] name servers can respond with the answers.

So that's why we have this concept of primaries and secondaries. And then the primary name servers in the primary name service [inaudible] administrators, the DNS administrators, they would maintain the DNS databases simply in a technical term, [inaudible] zone five. So we ride the zone five.

And then these zone fives has to be transmitted or transferred to our secondaries so that we can maintain the consistency between primaries and secondaries. And then we also have those recursive name servers or caching name servers that we discussed. Usually the clients, when you query for a website, when you send an e-mail and so on, to find that answer, find the IP address, or the expected answer you would go and talk to these caching servers. And then in terms of the caching servers, as we discussed, they would go and talk to root name servers, the TLD name servers, and finally they would arrive at these authoritative name servers, which is our primary and the secondary.

So the queries can come into those, get the responses from them, and then send the responses back to the client or the resolver. So in this process, there are a number of data flows and components that we can see. The question is where we are vulnerable. If someone wants to attack us, where can these attacks can be? So this is a question that we have to ask.

Unfortunately, we get attacked anywhere. In your DNS infrastructure, you can see that there can be various type of attacks can come, DNS is vulnerable. So, for example, the corrupting of zone files can happen, then impersonation can happen say, for example, if you are a primary, you are giving your zone files to your secondary. So how do you know whether you are talking really to your secondary? And if you are the secondary, how do you know whether you are really talking to your primary name server?

There could be always impersonation, someone can pretend to be you. There are dynamic updates so there could be some remote update can come into our DNS servers and get our DNS servers updated. So if we are expecting those remote updates, we have to make sure that we check the authenticity of those.

Then we have our caching servers, and I mentioned about cache pollution or cache poisoning type of attack. And then those type of data corruptions are also there. So that is why our DNS infrastructure, we have to analyze properly and understand which mechanism or which security mechanism we should use to protect our DNS infrastructure.

In this slide, you can see that some of the rows are shown in red. Some of the rows are shown in black. We have different type of security mechanism to protect those. We have primarily we have two types, one is called the server protection side and the other one is called data protection side. So the black arrows, you can see those black arrows in the places where we can use security mechanisms to protect our servers. Whereas in the red arrows, you can see, we can use those security mechanisms to protect our data.

Now here we'll see, okay, what is this data protection and what is the server protection? Now when we get the server protection, we are talking about two aspects again, one is obviously protecting our servers physically, right? So which means even to your data center, we have to have proper physical security and the login to your machines and things like that in our proper physical security aspects.

And then we also have another security mechanism in DNS. This is to protect server transactions. So this is called transaction signatures and this is an RFC [inaudible], request for command. So it's a standard and with TSIG in simply to identify this particular security mechanism. It's calling TSIG, or transaction signature. So TSIG can protect these server transactions.

So for example if you have a primary name server and if you have a secondary name server, the transactions happen between these primary and secondary name servers can be protected using these security mechanisms, what we call TSIG or transaction signatures.

And then the next security mechanism, which is very important, as well, that is to protect our data, so the data protection. That is the objective here. Now here the security mechanism we use is called DNSSEC. Maybe you have heard about the security mechanism quite a lot.

DNSSEC has been there for quite a while. People have been discussing about it quite for quite some time. There has been a lot of updates, discussions happening, as well.

This is to protect our data, so to achieve authenticity and the integrity of our data. Say for example, we want to visit a certain website, we want to know whether are we going to the right place, and also the integrity of this data. Are we really seeing the right, the correct data? That's what we want to achieve here in DNSSEC. These are security mechanisms that we try to achieve to protect our DNS infrastructure.

Now I would try to spend a little bit of time on DNSSEC or pay some emphasis here on DNSSEC because that's quite important. Here we use public key cryptography. Say, for example, with keys, this is a mechanism, which involves key, key-based security mechanisms.

Now when I say keys, we will have private keys and public keys. Say for example, if you want to really know whether this is my data, how can you verify that it's really my data, whether it's really me? So that can be done by using the signature or a digital signature. I will basically sign this data.

So I'm publishing some data, I will publish that data and I will sign that data. So I will sign those data using my private key. That's why actually I will have two types of keys. One is what we call a private key and the other one is what we call a public key. I will sign my data using my private key so that I will generate a signature for that and I will publish this signature.

But I will keep, I will make sure that I keep my private key safely. Others cannot see that because that's supposedly by private key. Now then how can then someone verify whether it's really my signature? That can be verified using my public key. For that, I have to publish my public key, as well, so I would publish my public key and then, also, I would publish my signatures that are associated with my data.

This is the basic mechanism in DNSSEC. So now you can see, if you refer to this slide now, if you refer to that previous DNS query process that I went through, the same thing happening just like before, but only thing, only difference here is that all those answers now we are getting from those DNS servers, they are being verified using the signature. So there is a signature associated. So there is a signature attached to that information that I'm getting so that always ICANN verify that signature using the appropriate public key. So this is what we try to achieve in DNSSEC.

Okay, now quickly moving on to DNSSEC, which is again a very important security mechanism in protecting our DNS data. Now at the root – DNSSEC actually understood, DNS is a hierarchy. So you have root, then you have TLD, then you have next level, and so on. So to verify this whole security mechanism or the verification process, we have to go all the way to the top. So that means say, for example, if the child has to pass this propagation of trust, basically, to its parent, and then the parent has to pass that to parent's parent and so on, and all the way up to the root. So that's why the root zone has been signed. And we have key for the root zone.

So this whole channel has to be fulfilled so that we can have that verification process. The root has been signed. The next level after that is the TLD level. In the TLD level, ICANN, I'm showing a map here. This is actually a map of ccTLDs, the country code top-level domains in the world, who have signed their zone or we can say DNSSEC deployed. So all those green areas you can see the countries in those green, they have deployed DNSSEC, they have signed their zones.

So that means actually the domains below that, they can also sign their zones and send or propagate the trust to its parent because of ccTLD. And then ccTLD can propagate the trust to the root, right? So that's how the mechanism works.

Now these also some [inaudible] that you can see, this is at the TLD level. So you can see that about 80% of the TLD today, they have signed their zone, so that means deployed DNSSEC, so about 80% of those. But beyond that, it's not much. It's a very small percentage. The second level domain, it's a very small percentage.

The graph you can see that in the last three years, we saw a big jump, the curve. The curve has been very sort of lenient in before 2013, but after 2013, you can see the curve is fairly steadily growing because in the new RAA, the Registrar Agreement DNSSEC or the [inaudible] Registrar Agreement the DNSSEC is already there as a requirement there, so that is why you could see especially the new gTLD [inaudible] and so on, they would deploy DNSSEC, and we can see more and more TLDs are deploying DNSSEC now. So this is from a statistical point of view, for you to think about.

Now you could be from enterprise level, you could be from, say, financial institutions, universities, or other enterprises and organizations and so on. Now if you're from such organization, something to think about, have you really signed or deployed DNSSEC at your level in your zone?

Sometimes when we speak to a lot of these enterprise level or second level type of owners, we see that they would respond, they say [inaudible] sometimes our technical staff, they are not still capable of handling DNSSEC. Sometimes they would say, "Okay, we are not ready yet." There is still some fear, uncertainty, and doubt about DNSSEC, maintaining DNSSEC, and so on. Also sometimes we hear that clients would tell that okay, our ISP is not providing that, they're not actually doing the validation, so we can't really do much, and then but when we ask the ISPs or the operators, registrars, and so on, they would say that, I mean, our clients are not really asking about it, so we don't see much of a demand there.

So this is something kind of a chicken and egg situation, as well. So it's certainly for you to think about what sort of difficulties you have. Bottom line is that it's a very important security mechanism for you to implement, at least start from now, start from a test environment. You don't have to go tomorrow and try to do it in a production environment. You can always try to attend training courses. ICANN do offer training courses on DNSSEC. There are various other organization bodies who offer DNSSEC workshops training courses, as well. So try to gather knowledge about these security mechanisms and then try to implement DNSSEC in your organizations in your zones and domains.

Okay, now let's actually spend a little bit of time on trying to focus a bit more onto handling DNS abuse. So we had a discussion about DNS security and so on. Now if our DNS infrastructure is not safe enough, miscreants, the attackers, and so on, they can use our DNS infrastructure for various sort of abuses.

There are lots of common uses for registering malicious domains. These domains can be used to sell counterfeit goods or various data exfiltrations or to launch some attacks, sell various illegal pharmaceuticals, and so on, malware command and control, phishing type of attacks. We normally get e-mail scams and so on, right? There are lots of 419 type scams.

So all these are done because if our DNS infrastructure is not safe enough, and people, miscreants try to abuse those services and infrastructure. Now also actually, they can abuse the miscreants, they can abuse other people's domain and DNS infrastructures, as well.

So for example, without you knowingly, your DNS infrastructure can be used by them. They could use your DNS servers. They could use your mail servers. They can use your name servers, and so on. They can change the configurations so that earlier we discussed some of those type attacks, as well, so your queries are going to your DNS name servers, they could be receiving those DNS queries. So these are various type of abuses that the miscreants attackers then they can launch.

And sometimes the abusers, they can acquire these DNS resources by various ways. They can, for example, they can use, they can purchase domain names by using stolen credit cards or some compromised accounts. Sometimes there are lots of free services available. They can use, they can abuse these three services available for in case if you're providing some free services, this is something to think about because lots of miscreant attackers, they would go and get domain names in free [inaudible] and so on.

And so leverage proper bulletproof, what we call bulletproof or gray hat hacking. [inaudible] provide they can use them to exploit them. Also, actually, they can hack legitimate hosts, as well, as I mentioned to you before. And also, sometimes when we deal with our domain name accounts, our registrars would provide us a Web interface, Web account for us to manage our credentials, details, and so on. So the attackers can get work credentials by various way and they can try to change our name servers inside those profiles, inside those portals, and so on, and then they can actually try to get control over that. So these are various ways how the abusers they can actually use our DNS resources, as well.

So when we in the organization level, if something happens, if we are going to handle these abuses, it's always good to pay attention to some of those items such as listed in this slide, say, for example, in the Whois database [inaudible] detail, privacy protection service details, because if there are some privacy protection service providers, try to evaluate them and get their details [inaudible] want to handle some incidences, values related to your DNS zone files, zone data, details about your DNS name servers.

Sometimes if you do some abuse handling, if you find some suspicious DNS name servers and suspicious hosting locations, always these are things that you should try to find more information about. So all these listed items are quite important when we handle DNS, even your mail headers, if you are trying to analyze different mails and so on, try to go and check the mail headers and what are the suspicious looking ones and so on.

So I think these points that's what we discussed so far, focuses on the DNS security, different security mechanisms, DNSSEC, and so on, and also DNS abuses. So at this point, let's try to stop for a little while and take a pop quiz. And Yesim, over to you.

YESIM NAZLAR: Thank you very much, Champika. Yes, we do have some pop quiz questions for you. They'll now appear on the right hand side of the screen.

CHAMPIKA WIJAYATUNGA: Okay. It's interesting, actually, the question was – let me go to the question. The question is actually securing DNS is important because. I can see no one actually takes the first one, domain names can be spoofed. In fact, it is one of the reasons, all right? And there are multiple correct answers here. So first one is a correct answer because domain names can be spoofed and that's why securing DNS is important. I told you like you can go in the wrong website and so on, the domain names can be spoofed. Caches can be poisoned. I think we discussed that, as well. Some people have answered that correctly. Yes.

Now third one is DNS is a centralized database. Unfortunately, this is wrong. I can see that there are a number of people who have answered that because DNS is really centralized database. DNS is a distributed database, so it's a correct answer.

And D, DNS servers can be impersonated, yes. So whoever responded that, that is a correct answer. DNS servers can be impersonated. And then the last one is none of the above, which is not correct. So the correct answers are A, B, and D. I think we can go to the next question.

YESIM NAZLAR: And Champika.

CHAMPIKA WIJAYATUNGA: Yes.

YESIM NAZLAR: Sure, Champika. Apologies for not being able to read out the questions because I lost my connection and quickly, I'll move on to the second question.

CHAMPIKA WIJAYATUNGA: No problem.

YESIM NAZLAR: The second question is what's the main objective of DNSSEC? A, protecting DNS data. B, protecting DNS servers. C, protecting both DNS data and DNS servers. C, increasing DNS queries. D, none of the above. Please cast your votes now.

CHAMPIKA WIJAYATUNGA: I think the comment here that you cannot choose more than one answer. Maybe it's not tick box, it's probably [radio] button, maybe that's why. I think that's a bit of technical glitch there but yeah. The answers are supposed to be yes. There can be more than one answer. Sorry if you cannot tick more than one answer, though.

Okay, let's try to evaluate that. So the question is what is the main objective of DNSSEC? As I mentioned to you before, the main objective of DNSSEC is to protect the DNS data. Right? So the correct answer is A. Protecting DNS data. The second one is protecting DNS servers. That's not really achieved or that's not objective of DNSSEC. I told you there are other security mechanisms like TSIG and so on, so that is to protect our DNS servers.

So the C is also not correct because it's not to protect both DNS data and DNS servers. And then the D is encrypting DNS queries. No, we are actually not encrypting DNS queries here because in our DNS data is all public data, so we are not really encrypting that. So that's not the correct answer, either. So the last one is also not correct, that is none of the above. That's not correct, as well.

Okay. I hope that that gave some understanding. So now I will actually quickly discuss the next few slides on with regard to DNS abuse handling. Now there are various tools and techniques and also we can contribute to some of the policies and guidelines in terms of handling DNS abuses. So when you handle DNS abuses, there are a number of resources that can be useful. Say, for example, the domain names. Domain names are very much useful because these are all Internet identifiers.

Then the IP addresses. IP address is also very important because that's also an Internet identifier, one of the primary Internet identifiers. AS numbers are what we call autonomous system numbers. So these are all quite new resources. Now there are various tools that can find more information about these identifiers because when we try to find the source, say, for example, where are these, who is abusing these? From which networks these abusers have? Or from which registrar who actually has given these domain names? Things like that.

So always finding more information can be always helpful. Whois database is one of the very important resources that you should look into in terms of tools, and also there are various other tools available, especially if you're working more in a technical environment, there are tools where you can use in different operating systems and so on. You can find more sophisticated details, especially for organizations like law enforcement and so on. Whatever the case, actually, if you're finding more details using these tools, it's always good to keep a record because the miscreants, they would actually, they would not keep these information for very long time.

So what you find today may not be available tomorrow or what you find now may not be available in the next ten minutes possibly, right? So that's why it's always, it's a good practice to keep record of what you do, what you find. At least try to document those. Keep some logs of those. Save the logs. These are always useful.

From a policy perspective or guidelines perspective, it's always important to talk to correct parties or get involved with the policy development processes when collecting abuses. You can deal with registrar. If you are dealing with registrars, domain operators, ISPs, and so on, accessible use of policies are very important to look into because usually these are sort of operators, providers, and so on, they should actually provide their policy in AUP.

Whois database and security is quite important, dealing with national third law enforcement, ICANN compliance is also very important. From ICANN perspective, there are various working groups, there are various Whois working groups, public safety working groups, and so on, that you can contribute to these policies and processes, as well.

So I think now at this stage – let us actually go to our other presenter, my friend Kitisak, who will discuss some of the case studies that he normally handles in an operational environment so that you get a practical understanding, as well, to these aspects.

KITISAK JIRAWANNAKOOL: Okay. Thank you, Champika and hello, everyone. My name is Kitisak Jirawannakool, I would like to share you about recent cases in Thailand.

Well, actually for you, two cases. The first case is, the scenario is a one day when we [inaudible] monitor our system and we find something, [inaudible] our dashboard.

We use [inaudible], which is an open source tool for monitoring performance of server. And user cannot resolve domain name for the domain name because of DNS server that's not worked properly. When we look to the percentage of [inaudible], it's high and also [suing] quickly, and then we check under the session after server is pretty normal.

Then when we investigate more, we monitor at the [inaudible] when we check, and if far there are too many list requests from many sources and also our mechanization [inaudible] this is DNS [inaudible] attack. And also IP address offer attacker IP address are spoof, and you cannot track the new attacker.

But we have to learn the pattern of attacker. For example, [inaudible] IP for country. Fortunately, in my case, [our first] IP came from only one country and I use [inaudible] to check randomly the country of the IP address. This case is consume all resource of DNS server is, of course, these are the DDoS attack. So then this [inaudible] for attack, this is a case that attacker spoof IP address and send many requests with every type of [inaudible].

For example, attacker want to attack by sending query [inaudible] with a [inaudible] or MX type and A type, as well. What did they do to respond this case? First thing [we do there] based on different criteria, the group of IP address or country. And also we add the white list to allow only our client be able to solve domain name.

This one need to be consideration about organization policy, as well. Iin some cases, attackers send requests by using nonexistent domain. We have to locate this type of request, too. The second scenario we monitor our [inaudible] and [inaudible] there are several queries request from [client] to outside. That mean the client didn't use our data server.

The signature of the [inaudible] this are more thorough DNS request traffic and, of course, they [text back] by our [inaudible] already. When we find more information and we found that model is a type [inaudible] botnet and itself send command through query request. It looks like a normal DNS query we have here.

So this is the explanation of this kind of attack. Usually got infected by [inaudible] and send a command through the DNS record to the CnC server, which is DNS server outside of organization. How can you respond? If you find request from outside, that mean possibly your DNS server have and use it as a CnC server. In this case, we need to pass and [inaudible] the servers.

The second choice, actually that mean if you find request to outside, it's possibly your client got infected by malware so you need [inaudible] antimalware security. And also for the management level, we have to create the internal policy and, of course, we have to work with other firm and find the best solution to fight against this kind of malware. So these are [inaudible] my presentation so I need to pass back to Champika.

CHAMPIKA WIJAYATUNGA: Okay. Thank you, Kitisak. Now we have come to the last of these webinar. Now this is more about collaboration with ICANN. Now in ICANN, we have a team or we have a program, SSR. SSR stands for Security, Stability, and Resiliency Team. Now SSR Team actually we deal with many of these type of secure issues, many of these actually incidents and so on.

So the collaboration with SSR related work with ICANN is very important. Now you may be coming from various organizations. You can see this in the slide. We do work very closely with, say, for example, governments, the law enforcement bodies, the domain operators, the regional Internet registries, the national [thirds], the network operators, and so on. There are a number of other parties, as well.

So if you belong to these sort of groups, always you can be involved with SSR work with ICANN. So trust-based collaboration is something that we can always achieve to make sure we can always achieve to make the Internet secure, stable, and resilient, and keep it very healthy.

Training and outreach is also something that the SSR team provides. If you think that there are some capacity building that you need, in fact, we discussed before, if the organization, if your communities would like to have some more in depth maybe hands on type training on security, DNS, DNSSEC, DNS abuse handling, and so on using those tools that we discussed and so on, we can always support you, assist you, and so on.

Do try to be involved, work with us, collaborate with us, and also ultimately contribute to those policies that we discussed, and to those working groups that what we mentioned. This is what actually what we wanted to wrap up, and finally, we have a very quick pop quiz. Maybe you can take a minute or so to do this.

YESIM NAZLAR: Hi, Champika. Sure. Let's move on to our third question then. Our third question is following evidences can be helpful to handle DNS abuses. Questionable [inaudible], notorious name servers, frequently involving users, suspicious mail headers, all of the above. Please cast your votes now.

And the correct answer, Champika or the answers maybe.

CHAMPIKA WIJAYATUNGA: Okay. I think everyone has got it correctly over there. Mostly most of you I think. The question [inaudible] is that A, B, and D quote. Yeah, so it's always now helpful to have those questionable Whois data, the [inaudible] name servers, and the suspicious mail headers. Not really the number C, which is frequently browsing users, and then E is not all of the above correct, either, because C is not correct.

We can quickly go to the next question, the last one.

YESIM NAZLAR: Sure. [inaudible] the last one is policies and guidelines with regard to following [inaudible] enhance the efficiency of handling DNS abuse. Evidence collection, dealing with registrars, dealing with national CRTs, coordination with law enforcement bodies, none of the above. Please cast your votes now. And the correct answer, Champika, is.

CHAMPIKA WIJAYATUNGA: Okay. As we can put multiple answers, actually, A, B, C, and D are correct. So not the last one, none of the above is not correct, so A, B, C, and D are correct because you can, obviously, you can work with them, right? All those mentioned authorities, mentioned entities, and you can contribute to the policies and guidelines, as well.

So I think thank you very much. I think that wraps up our presentation, our webinar for today. So just to mention about the summary, so we started with the threats and risks in DNS, I mentioned in both possible very commonly type of attacks that we see in DNS, and then I mentioned why the DNS security is important. I talked about those different security mechanism, protecting DNS servers, protecting DNS data. We talked about DNSSEC, as well, a little bit in detail, then we had a chat about DNS abuse handling, how the miscreants they can use our DNS resources, and then we mentioned about tools and techniques to talk about some case studies and finally the collaboration with ICANN and with some quizzes.

I hope this session has been useful to you and if you have any questions, we can spend a few minutes in case if you have any questions.

KELVIN WONG: Thank you so much, Champika, and also thank you so much, Kitisak. It was very informative. I know that we are past the hour so I'll hand over to Silvia to take over for the Q&A [inaudible].

SILVIA VIVANCO: Thank you very much, [inaudible] and Champika and Kitisak. Excellent presentations. Please, if you would like to ask some questions, raise your hand or you can type it on the chart and I will read it for our presenters. I'm checking now the chat. I do not see any questions at the moment. I'm just responding to Holly, yes, the presentations are already put on the wiki page on this meeting's wiki page. So you can download the presentations and you will be able to listen to the recording, as well.

I have a question from Maureen Hilyard. Is SSR related to SSAC? I think this is for Champika.

CHAMPIKA WIJAYATUNGA: Okay. SSAC, SSAC stands for Security and Stability Advisory Committee. So that is actually an advisory committee that is in the ICANN, you know, within the ICANN community, right? In ICANN's framework that the advisory committee basically provides advisory to the ICANN, and there are [inaudible] SSR is team within the ICANN operational, within the organization and that involves.

In fact, we work closely with SSAC, as well, and also to work closely with the community and to deal with the SSR or security-related matters and contend, do capacity building, and engagement, as well. So that's the sort of difference whereas SSR is a function of ICANN, whereas SSAC is an advisory committee.

SILVIA VIVANCO: Thank you very much, Champika, for this very useful information. I see no further questions, let me check. I don't see any hands at the moment. Okay. So I believe we now have additional questions. But of course, if you are interested, you can always send an e-mail to the presenters and they will be happy to reply and At-Large staff will be happy to convey those questions to the presenters. So if you have more questions for later on, please feel free to e-mail us with those.

And now I will turn it over to Yesim to start an evaluation survey. So please be so kind to explain with us just for four minutes to complete the evaluation survey. Go ahead, Yesim.

YESIM NAZLAR: Thank you very much, Silvia. Let's make quickly go over these questions. First question is the [inaudible] feature of those Adobe Connect room is part of the pilot. Please choose [inaudible] terms: very helpful, helpful, less relevant, not helpful. Please cast your votes now.

Thank you very much. I'll now quickly move on to our second question. Please help identify all categories that describe who you are. A person with disabilities, participant for whom English is a second language, participant who doesn't speak English, participant who has limited or low bandwidth. None of the above. Please cast your votes now.

Thank you very much for this one, as well. Moving on to our third question. What benefits did you get from accessing the captioning stream? Choose as many answers as possible. Great understanding of the topic, ability to understand the session more effectively, provided the correct spelling of technical terms and terminology, personal benefits of being appreciated, and [inaudible] more fully participate and engage with the presenter. Please cast your votes now.

And quickly moving on to the next question. What benefits did you get from accessing the captioning stream? If there are any other than we have just mentioned before, please type your answers here in the blank space and please do not forget to click on the icon just next to it in order to send the answers.

I'll be waiting for a short time for the answer. Here we are. We have one already. Thank you very much. Let me move on to next question then. Where else do you think captioning should be required? Working groups, taskforces, ad hoc groups, RALO calls, ALAC calls, CCWG calls, and other constituencies. Please cast your votes now and remember you can choose more than one option here.

Thank you very much for your vote. Let's quickly move on to our fifth question, the next question. How do you rank today's session in terms of quality of information? Please vote from one to five, one as very poor and five as very good. Please cast your votes now. Thank you very much. Moving on with the next question.

How was all the presenters' delivery? Please cast your votes now, one as very poor, and five as very good.

And quickly to our question number eight. Do you plan on using any information directly with our At-Large structure? Please cast your votes now. It's a yes or no question. So for the ones who have answered as yes, we have a following question for you here. If yes, please explain. Again, please type your answers in the blank space and do not forget to just click on the icon next to it so we can all see the answers. Recommendations about the content of the session. Please type your answers in the blank space, and again, please do not forget to click on the icon next to it for both the answers.

CHAMPIKA WIJAYATUNGA: Okay. Actually, I have put my contact detail at the end of the slide. So feel free to send an e-mail or talk to any of our... Actually, we have a customer service help desk, as well, in the APAC Hub. You can write to them, as well, and they will be in touch with me, and then depending on your requirement, we can obviously have some further discussions.

YESIM NAZLAR: Thank you very much, Champika, and this was the end of the survey questions. So over to you, Kelvin? Would you like to add any more?

KELVIN WONG: Okay. Sure. Okay, thank you. All that's left for me to say is to thank these speakers, Champika and Kitisak, and all the feedback that we have received as a testament to the good work that you have done. And also thank you to the At-Large team of Silvia and Yesim for putting this together. So and thank you, of course, to everyone who have stayed with us until now and completing the survey, which is very important to us.

So I'll close this webinar and return you back to your work. See you, everyone. Bye-bye.

UNIDENTIFIED MALE: Thank you, all. Very nice talking to you all.

UNIDENTIFIED FEMALE: Bye.

UNIDENTIFIED FEMALE: Thank you. Bye-bye.

UNIDENTIFIED MALE: Thank you all. Bye-bye.

YESIM NAZLAR: Thank you, everyone. [inaudible]. The recording will now be disconnected.

[END OF TRANSCRIPTION]