FINISHED FILE
ICANN
MAY 17, 2016
12:00 A.M. CST

Services Provided By:

Caption First, Inc.
P.O Box 3066
Monument, CO 80132
1-877-825-5234
+001-719-481-9835
Www.Captionfirst.com

***

This is being provided in a rough-draft format. Communication Access Realtime Translation (CART) is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.

***

>> YESIM NAZLAR: Welcome everyone. Welcome to all of those who have been joining. We are currently gathering. Can we have two more minutes to start for the scheduled start time? Thank you.

Welcome to all of those who have been joining. We are currently still gathering and we will be waiting for three more minutes more. Thank you very much for your patience. Just remind everyone that if they are not speaking they should mute their video. We have a rather windy noise coming from someone.

>> KELVIN WONG: Okay. Hello everyone. Can you hear me? Okay. Welcome to the APRALO capacity rating seminar. This is Kelvin Wong from the Impact Hub and also from the large staff supporting this. Just to give you a background, the webinar series is an initiative under the APRALO APAC hub for integration framework where topics are collaboratively decided on together and we have been doing this for awhile, about five months and other topics have included international domain names and Internet governance. Today the topic is DNS security and DNS abuse webinar. If you recall last July we had a DNS basic and DNS ecosystem webinar which is done by Shen Shang. It is a continuation to that. Our speakers for today would be Champika and Kitisak. Champika is ICANN -- he is a big part of ICANN's global

engagement and represents ICANN in running workshops.

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 different areas. And also awareness raising. Furthermore, he has improved security for many government organizations and he conducts many training classes related to information security, especially IT security awareness. I think we are in very good hands. And before we start the webinar proper I will hand over to Hann Kenn, our new GSE for APAC hub which will go over the housekeeping rules. Over to you, Hann Kenn.

>> HANN KENN: If you have any questions please raise them in the port to the left. Questions and answers will be posted on the webinar's Wiki page. Okay. There will be a pop quiz after each segment. So do be ready to answer the questions posted in the poll chart in Adobe Connect. At the end of the webinar please remain on the call for three minutes to answer a short survey. Your feedback will be essential in improving our webinars to your needs. Now thank you for your attention. I will hand it over to Champika.

>> SILVIA VIVANCO: Hi this is Silvia speaking. Champika, would you like to go on and start? Champika, can you hear us? Okay. I believe Champika has lost the audio and the connection. So please bear with us and let us give just one, two minutes for him to log back in. Thank you very much for your patience. Champika, can you hear us now?

>> CHAMPIKA WIJAYATUNGA: Hello. Can you hear me?

>> YESIM NAZLAR: Yes, we can hear you, Champika. Please go ahead.

>> CHAMPIKA WIJAYATUNGA: All right. Okay. Yep. Thanks very much. And sorry for the little interruption. I suddenly lost my Adobe Connect screen. Without taking much time thanks very much for the introduction. And so today's session as we all know it is going to be on 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 especially want to acknowledge Deb Skittlo, VP and IT coordination at ICANN and Richard Lamb. They have contributed to these materials.

The agenda that we are planning to do today we are going to discuss threats in DNS and later will discuss why the DNS security is important. We will spend a little 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, especially focusing on the SSR or security stability and resilience aspects.

Let us have a look at threats in DNS. As you know we had another session earlier 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 product and it is very important for us to understand, especially focusing the DNS aspects. Now here you can see that in the slide there are a few components. First of all, we have a client, this could be a user device basically. That in this case it is sort of browsing a certain domain name. In this case it is www.example.net. 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 Web page. So when the client sends a 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 you are at home, in a residence, it could be ISP that provides that. If you are in a work environment maybe your organization is providing this service. So usually this sort of service or the server that provides the service is called a recursive server or resolver or a patching server. Now that server gets the request from the client and then sends a request to root servers. There are a number of root servers scattered around. The requests will go to the root servers and the root server will give a response or a sort of reference to talk to the next level. As we all know in the DNS hierarchy the next level is the TLD level. So in this example the TLD level is dot net. So the reference comes from the root server to go and talk to the dot net name server. And then the recursive server or caching server will talk to the dot net name server and ask the same questions. I need the IP address of www.example.net. And then dot 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 recursive server gets that information and goes and contacts the authoritative server related to that example.net zone and gets the relevant or connect web server IP address.

So the authoritative answer comes from the main server example.net. It could be one name or they could be having multiple names. Once the resolver or caching server gets the answer that answer will be passed on to the client. So 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 Web page. This is how the simple DNS query gets resolved. So now moving on -- now the next slide here should be in that process we saw that there have a number of components that we saw. We had resolver recursive servers. We had root servers and other name servers like authoritative name servers and so on. Now in this DNS ecosystem all these DNS name servers, there were some certain risks that we encountered. One of the common attacks called reflection attacks. Now when the client sends a request to these recursive servers they are given sort of a question to go and find and then respond 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 their client and then send that request to the recursive server, then unfortunately the recursive server instead of replying to that client who really asked the question if you respond to the spoof identity. This is where these sort of reflection and amplification attacks would come.

In the case of amplification attacks the answer is quite big in size. So the bandwidth will be highly utilized. Now this can be actually in the form of what we call DDoS attacks or distributed denial of services or reflection and amplification. The attacker could control a number of or send a number of queries, requests to a number of these 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 it is you except the queries only from your clients. But there are lots of networks out there who would or the DNS servers, these recursive name servers would accept the queries not only from the 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 fend 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 and bandwidth will be utilized and processing power would be utilized and the servers can crash. These are some of the common threats that we have.

Cache poisoning is another DNS threat. Thus what happens if you remember that recursive DNS that we discussed, once it gets these answers it keeps the answers in its memory or in the cache. So the next time when a client asks a similar type of question, the same question it can respond to that other client in a very quick way. Because it doesn't now have to go and talk to routine servers or other authoritative named servers. So the answers can be quickly. This is because they keep cache -- they keep those answers in the memory. Unfortunately if someone tried to poison this cache then the recursive servers can answer or give wrong answers, they can behave differently and give wrong answers. There is what we call cache poisoning. Sometimes some attackers, can try to create, go and buy a domain name and create some, you know, domain name or a website and then they could actually get their 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 DNS named servers. So the caching server memory or can keep wrong answers related to others. These are all threats that happens in the DNS space. So cache poisoning is something that happens very commonly.

There is another common threat which is what we call DNS highjack or query interception. Usually when the DNS queries have been asked

by the servers if the attacker hacks in to a DNS server itself or to the router access point, somehow the objective here is that they would redirect the query in to one of the DNS servers or the recursive servers controlled by them. So that they can instead of answer -- instead of query being answered by the correct genuine DNS server now the query is being answered by the attacker. They can always redirect you. If you are looking for www.example.net they can redirect you to a Web page that goes to a wrong website hosted by the attacker basically. And sometimes, you know, if 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 credentials 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. So, for example, if we have a domain of -- we have a zone called example.net, the administrators of that zone would name a primary name server to provide that name service for example.net. In case if we only have a primary name server, in case an attack comes to a primary, if that goes down then there is no redundancy. That's why we have to have another redundancy or multiple or what we call secondary name servers. If one of the main servers is down the secondary can respond with the answers. That's why we have these concept of primaries and secondary. The primary name servers, DNS administrators they would maintain the DNS databases. Simply technical terms we call those as zone files. So we write the zone files and then these zone files have to be transmitted or transferred to our secondaries so we can maintain the consistency between primaries and secondaries. And then we also have those recursive main servers or caching name servers, when you send an e-mail and so on find the IP address or the expected answer you would go and talk to these caching servers. And then in turn the caching servers we would talk to root name servers and TLD and they would arrive at these authoritative name servers which is primary and secondaries. So the queries can come in to those and get the responses from them and then send the responses back to the client or the resolvers. 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 these attacks can be. So this is a question that we have to ask. Unfortunately, we can get attacked anywhere.

In your DNS infrastructure various attacks can come. So, for example, the corrupting of zone files can happen. Then impersonation can happen. 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 things called dynamic updates. So there could be some remote updates can come in to our DNS servers and get them updated. If we are expecting those remote updates we have to check the authenticity of those. I mentioned cache poisoning type of attacks and then those type of data corruptions are also there. 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 arrows are shown in red and some of the arrows are shown in black. So we have different types of security mechanisms to protect those. We have -- primarily they 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 will see okay, what is this data protection and what is the server protection. Now when we get to server protection, we are talking about two aspects again. One is fiercely protecting our servers physically. So which means, you know, even to your data center we have to have proper physical security and, you know, the log in 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 request for connect. So it is a standard and we call TSIG to identify this prior security mechanism. It is called TSIG. So TSIG can protect these server transactions. If you have a primary name server and a secondary name server the transactions that happen between these primary and secondary name servers can be protected using these security mechanisms what we call transaction signatures. And the next one 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 this security mechanism. DNSSEC has been there for quite awhile and people have been discussing about it for quite some time. A lot of updates and discussions happening as well. So this is to protect our data, to achieve authenticity and integrity of our data. If we want to visit a certain website, are we going to the right place. And also the integrity of this data are we seeing the correct data. That's what we want to achieve here. 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 place some emphasis on DNSSEC because that's important. Here we use public graphy. For example, we have keys. This is a mechanism that involves key-based security mechanisms. 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 is really my data, whether it is really me. So that can be done by using the signature or digital signature. I will basically find this data. So if I am publishing some data I will publish that data and I will sign that data. So I will sign those data using my private keys. That's why actually I do have two types of keys. One is what we call a private key and the other one is what we call a public key. So I will sign my data using my private key so that I will generate a signature for that. And then I will publish this signature but I will make sure I keep my private key safely. Others cannot see that because that's supposed to be my private key. Now how can then someone verify whether it is really my signature. So that can be verified using my public key. So for that I have to publish my public key as well. So I would publish my public key and I would publish my signatures that are associated with my data. So this is basically the mechanism in DNSSEC. 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 have been verified using the signatures. So there is a signature associated. So there is a signature attached to that information that I'm getting. So that always I can verify that signature using the appropriate public keys. So this is what we tried to achieve in DNSSEC.

Okay. Now quickly moving on to DNSSEC which is a very important security mechanism in protecting our DNS data. Now at the root -- now DNSSEC, as we understood DNS is a hierarchy. So you have root. Then you have TLDs and 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 a child has to make it passed this propagation of cusp to its parent and the parent has to pass that to a parent's parent and so on and all the way up to the root. So that's why we -- the root zone has been fine. And we have keys 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. So the next level after that is the TLD level. The TLD level I can -- I am showing a map here. So this is actually a map of ccTLDs, the country code top level domains in the world who assign their zones or we can DNSSEC deploy. All the 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 which is a ccTLD and ccTLD can propagate the trust to the root. So that's how the mechanism works. Now there is also some statistics that you can see. About 80% of the TLDs today they have signed their zones. That means deployed DNSSEC. About 80% of those but beyond that it is very, you know, it is not much. It

is a very small percentage. The second level domain, it is a very small percentage. The graph you can see that in the last three years we saw a big jump. The curb, the curb has been very sort of lenient in before 2013, but after 2013 you can see the curb is steadily growing because in the new RAA, the register agreement, the DNSSEC is already there as a requirement there. So that is why you can see especially with the new gTLD they would deploy DNSSEC. And we can see more and more TLDs are deploying DNSSEC now. This is from a statistical point of view for you to think about.

Now you could be from an enterprise level, you could be from say, you know, financial institutions, universities, or other enterprises and organizations and so on. Now if you are from that organization -- such organization, something to think about, have you really signed or deployed DNSSEC at your level in your zone. Sometimes when you speak to a lot of these, you know, enterprise level or second level type of owners, we see that, you know, they would respond they say sometimes our technical staff, they are not still capable of handling DNSSEC. Sometimes they would say okay, they are not ready yesterday. There is still some fear and uncertainty and doubt about DNSSEC, maintaining DNSSEC and so on. Also times we hear that, you know, clients would tell that okay, your ISPs is not providing that. They are not actually doing the validation. So we can't really do much. And then but when we asked ISPs or 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. It is something for you to think about what sort of difficulties you have. Bottom line is that it is 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. And there are various other organization bodies who offer DNSSEC workshops and training courses. Try to gather knowledge about this security mechanism and 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 on to handling DNS abuse. So we had a discussion about the DNS security and so on. Now because our -- if our DNS infrastructure is not safe enough, the attackers and so on can use our DNS infrastructure for various sorts of abuses. There are -- we can see there are lots of common uses for registering malicious domains and they can be used to sell counterfeit goods or various data exfiltrations or to launch some attacks, sell various illegal pharmaceuticals, phishing kind of attacks. There are lots of 419 such scans. All these are done because if our DNS infrastructure is not safe enough, and people trying to abuse those services and

infrastructure. Now also actually they can abuse the other people's domain and infrastructure as well. For example, without 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 discuss some of those attacks as well. Your query instead of going to your DNS main servers they could be receiving those DNS queries. So these are various types of abusers that the misscreen attackers and then they can launch and sometimes, you know, 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 compromised accounts. And sometimes there are lots of free services available. They can use -- they can abuse these free services available. In case if you are providing some free services this is something to think about because lots of misscreen attackers they would go and get domain names in free registrations and so on. And also leverage, you know, proper bulletproof, what they call bulletproof or gray hat hosting. And also actually they can hack legitimate hosts as well.

And also sometimes when we deal with our domain name accounts our registrars would provide as a web interface, web account for us to manage our credentials, details and so. So the attackers can get our credentials by various ways and try to change our main servers within those files and portals and they can try to get control over that. Various ways that abusers can use our DNS resources as well. So when we in an organization level if we are going to actually -- if something happens, if we are going to -- if we are going to handle these abusers it is always good to pay attention to some of those items that are listed in the slides. For example, in the WHOIS contact data detail, private protection service providers try to evaluate them and get their details in case if you want to handle some incidents, values related to your DNS zone files, zone data, details about your DNS name servers. Sometimes if you do abuse handling if you find some DNS name servers and suspicious hosting locations these are things that you should try to find more information about. All these listed items are important when we handle DNS abusers, even your mail headers. Try and check the mail headers and what are the suspicious looking ones.

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

>> YESIM NAZLAR: We do have some pop quiz questions for you. They will appear on the right-hand side of the screen.

>> CHAMPIKA WIJAYATUNGA: Actually securing DNS is important because I can see domain name spoofed, it is one of the reasons and there are multiple correct answers here. First one is a correct answer

because domain names can be spoofed and that's why securing DNS is important. Going in the wrong website and so on, caches can be poisoned. We discussed that as well. Some people have answered that correctly. Yes.

Now the third one is DNS is a centralized database. Unfortunately this is wrong. DNS is not a centralized data. DNS is a distributed database. So it is incorrect. And DNS servers can be impersonated, yes. And then the last one is none of the above. The correct answers are A, B and D. I think we can go to the next question.

>> YESIM NAZLAR: And Champika, apologies for not being able to read out the questions because I lost my connection. And quickly I move on to the second question. The second question is what's the main objective of DNSSEC. A, protecting DNS data, B, protecting DNS servers and C, protecting both DNS data and DNS servers and D, encrypting DNS queries and E, none of the above. Please cast your votes now.

>> CHAMPIKA WIJAYATUNGA: I think there is a comment here that you cannot choose more than one answer. Maybe it is not pick boxes. Probably it is radio buttons. Maybe that's why. I think that's a bit of technical glitch there, but yeah, the answers are supposed to be yes. There have been more than one answers. Sorry, if you cannot pick 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. So the correct answer is A, protecting DNS data. The second one is protecting DNS servers, that's not really achieved. That's not the objective of what DNSSEC is. I told you there are other security mechanisms, like TSIG and so on. So C is also not correct because it is not to protect both DNS data and DNS servers. We are not encrypting DNS queries. There is all public data. So again not really encrypting that. So that's not a correct answer either. So the last one also is not correct. None of the above, that's not correct as well.

Okay. I hope that gave some understanding. So now I will actually quickly discuss the next few slides on with regard to DNS abuse handling. There are various tools and techniques and also we can contribute to some of the policies and guidelines in terms of handling DNS abusers. So when you handle DNS abusers 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 and then the IP addresses. IP address is also very important because that's all Internet identifier, one of the primary Internet identifiers. AS numbers or what we call autonomous system numbers. These are quite useful resources. Now there are various tools that can find no information about these identifiers. We try to find the source, say, for example, who is abusing these, from which networks these abusers happen or from which registrar who actually

has given these domain names, things like that. So always finding more information can be always helpful. WHOIS data is one of the important resources that you should look in to in terms of tools. And there are various other tools available, especially if you are 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. And whatever the case, actually if you are finding more details using these tools it is always good to keep a record because the misscreens they would -- they would not keep these information for a 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 is always -- it is a good practice to keep a 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 guideline perspective it is always important to talk to correct parties or get involved with the policy development processors when collecting abusers. There are -- you can deal with registrars. If you are dealing with registrars, the main operators and ISPs acceptable use of policies are very important to look in to because usually these operators and providers they should actually provide their policy in AUPs. Who is your database and security is quite important. Dealing with national law enforcements. ICANN compliance is very important. There are various working groups, public safety working groups 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, you know, 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. Hello everyone. My name is Kitisak Jirawannakool. I am in Thailand. Actually I have for you two cases. The first case, the scenario is one day when we monitor our systems and we found something strange on our dashboard. We use Cacti which is an open source tool for monitoring performance of servers. And users can't resolve domain name, DNS doesn't work properly and percentage of CPU utilization is high and swing quickly and then we check at sessions of server is -- seem normal. Then when we investigate more we monitor at the firewall and we check and we find there are too many DNS requests from many sources and also our next generation firewall said this is DNS any queries brute force attack. And can't track real attackers because of IP address and cannot track real attacker but we have to learn the pattern of attacker. For example, proof of IP or country. Unfortunately in my case our first IP came from only one country. And they used database to check to their country of their IP address.

Consumed all resource of DNS server. This, of course, DDoS attack. So DNS, any queries brute force attack, this is a case that attacker spoofed IP address and send many requests with every type of when this occurred. For example, attacker wanted to attack by sending a query to abc.g.th or next type and A type. What did we do to respond to this case? First thing we filter based on different criteria, a group of IP addresses or country. And also we add whitelist to allow only our clients to be able to solve domain name. Consideration about organization policy as well. In some cases attackers send requests by using nonexistent domain. The second scenario we monitor our firewall and we find there are several queries, requests from client to our side. The client, they didn't use our DNS server. The significance of the firewall said this is Morto DNS request traffic and, of course, this action is blocked by our firewall already. When we find more information and we saw that Morto is a type of Internet worm and Botnet. And it send command through query requests. It looks like a normal DNS query behavior. So this is the explanation of this kind of attack.

User got infected by Morto worm and send a command through DNS server which is DNS server of our organization. How can we respond? If you find requests from outside that mean possibly your DNS server are hacked and use it as a C&C server. So in this case we need to patch and we need to improve security of DNS servers. The second, the second choice, need to find requests to our side. It is possibly your client got infected by malware. So we need to use anti-malware to clean it. And also for the management level we have to create the internal policy. And, of course, we have to work with other CERTs and find the best solutions to fight against malware. So this is all my presentation. So I need to pass back to Champika.

>> CHAMPIKA WIJAYATUNGA: Okay. Thank you, Kitisak. Now we have come to the last part of this webinar. Now this is more about collaboration with ICANN. We have a team or a program, SSR it stands for security, stability and resilient team. We deal with incidents and so on. So the collaboration with SSR related work that ICANN is very important. You may be coming from various organizations. You can see this in the slide. We do work very closely with say, for example, governments, with law enforcement bodies, domain operators and regional Internet registry industries and national CERTs and there are a number of other parties as well. If you belong to these sort of groups you can be involved with SSR work. 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, also some training and outreach is also something that the SSR team provides. If you think there are some capacity building that you need, in fact, we discussed before, if your 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 discuss and so on, we can always support you, assist you and so on. Do try to be involved and work with us and collaborate with us and also ultimately contribute to these policies that we discussed and to those work groups that what we mentioned. This is what we wanted to wrap up. And finally we have a very quick pop quiz. Maybe we can take a minute or so to do this.

>> YESIM NAZLAR: Hi. Sure. Let's move on to our third question then. Our third question is following evidences can be helpful to handle DNS abuses. Questionable WHOIS data, notorious name servers, frequently browsing users, suspicious mail headers, all of the above. Please cast your votes now. And the correct answer is, Champika, or the answers maybe?

>> CHAMPIKA WIJAYATUNGA: Okay. I think that everyone has got it correctly over there. Mostly most of you I think. The question -- the correct answers are A, B and D. It is always helpful to have those questionable WHOIS data and notorious name servers and suspicious mail servers. E is not correct because C is not correct. We can quickly go to the next question. The last one.

>> YESIM NAZLAR: Sure, here you are. Policies and guidelines with regard to the following can enhance the efficiency of handling the DNS abuse. Evidence collection, dealing with registrars, dealing with national CERTs, coordination with law enforcement studies, none of the above. Please cast your votes now. And the correct answer, Champika, is?

>> CHAMPIKA WIJAYATUNGA: Okay. 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 authority, 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 about some possible very commonly type of attacks that we see in DNS and then I mentioned to you why the DNS security is important. Talked about those different security mechanisms, protecting DNS servers, protecting DNS data. We talked about DNSSEC as well, a little bit in detail and then we had a chat about DNS abuse handling, how misscreens, we can use DNS resources and we talked about tools and techniques and case studies and finally collaboration with ICANN. Hopefully this session has been helpful for you. If you have any questions we can answer some questions.

>> KELVIN WONG: Thank you so much, Champika and also thank you so much, Kitisak. This was very informative. I know that we are passed the hour. And I will hand over to Silvia to take over the Q and A.

>> SILVIA VIVANCO: Thank you very much, Kelvin and Champika and

Kitisak for your presentations. Please if you would like to ask some questions raise your hand. Or you can type it on the chat and I will read it for our presenters. I'm checking now the chat. This is Silvia. I do not see any questions at the moment. Just responding to, 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. Is SSAC related to SSAC? This is for Champika.

>> CHAMPIKA WIJAYATUNGA: Okay. SSAC stands for Security Stability Advisory Committee. That is an advisory committee within the ICANN, you know, within the ICANN community. So within ICANN's framework the advisory committee provides advisory to the ICANN and the SSAC is a team within the ICANN operational, within the organization. And that involves, in fact, we work closely with SSAC as well and also work closely with the community and to deal with the SSR or security related matters and contents, do capacity building and engagement as well. So that's the sort of difference where SSR is a function within 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 don't have additional questions. If you are interested you can send an e-mail to the presenters and they will be happy to reply and our 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. Feel so kind to stay with us for four minutes to complete the evaluation survey. Go ahead Yesim.

>> YESIM NAZLAR: Thank you. Let me quickly go over the questions. The captioning feature of Adobe Connect room is part of a pilot. Please choose the suitable term. Very helpful, helpful, less relevant, not helpful. Please cast your votes now. Thank you very much.

I will move on quickly to our second question. Please self-identify all categories that describes 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. Greater understanding of the topics, ability to understand the session more effectively, provided the correct spelling of technical terminology, personal benefits of being appreciated and able to 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 others 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 answers. Here we are. We have one already. Thank you very much. Let me move on to the next question then. Where else do you think the captioning should be required? Working groups, task forces, 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 votes. 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 1 to 5. 1 as very poor and 5 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. 1 is very poor. And 5 is very good. And quickly to our question No. 8, do you plan on using any of the information directly with your at-large structures? Please cast your votes now. It is a yes or no question.

So for the ones who have answered 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. I am waiting for a few more seconds.

Okay. Here we have. I believe I can move on to our final question. Any further comments/recommendations about the content of this session? Please type your answers in the blank space. And again please do not forget to click on the icon next to it to post the answers.

We will wait a couple more seconds. Here you are. And I believe this is a question for you, Champika.

>> CHAMPIKA WIJAYATUNGA: Okay. Actually I have put my contact details at the end of the slide. So feel free to send an e-mail or talk to any of our, you know, 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 discussion.

>> YESIM NAZLAR: Thank you very much, Champika. And this was the end of the survey questions. So over to you, Kelvin.

>> KELVIN WONG: Sure. Okay. Thank you. All I need to say is to thank the speakers, Champika and Kitisak. And all the feedback we have received is testament to the -- and also thank you to the large team for pulling this together. And thank you, of course, to everyone who stayed with us until now and completing the survey which is very important to us. So I will close this webinar and return you back to your work. Thank you. See you everyone. Bye-bye.

>> CHAMPIKA WIJAYATUNGA: Thank you all. Very nice talk to you all.

>> Bye.

>> Thank you bye-bye.

>> Thank you all. Bye-bye.

>> Thank you, everyone. The recording will now be disconnected. Have a lovely day.

(Session concluded at 1:14 a.m. CST)

***

This is being provided in rough-draft format. Communication Access Realtime Translation (CART) is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.

***