KOBE – Joint Meeting: RSSAC and SSAC [C]
Tuesday, March 12, 2019 – 10:30 to 12:00 JST
ICANN64 | Kobe, Japan

RUSS MUNDY: Oh, Paul is back there. I had not spotted you.

UNIDENTIFIED MALE: [inaudible].

RUSS MUNDY: So in the session or the part of the session that deals with KSK, Paul's going to be leading that discussion. And as usual, this is a very informal meeting. We do have a set of slides this time, but it's more to help guide things along and move them along because there's not enough time to go over the slides in detail, and so that's the first important introductory pieces I want to add.

Since it's so full, I'm going to – unless somebody objects – just skip right into the agenda instead of doing intros, because there may be some people who don't know each other, but let's get going. We've got nine items in 90 minutes.

BRAD VERD: Raise your hand if you're RSSAC, raise your hand if you're SSAC.

RUSS MUNDY: Oh, well that’s a good one. Okay. Raise your hand if you're an RSSAC member. Raise your hand if you're an SSAC member.

BRAD VERD: There's a couple overlaps.

RUSS MUNDY: Yeah.

BRAD VERD: Who didn't raise their hand? Okay, good.

RUSS MUNDY: Paul. Okay.

SUZANNE WOOLF: I think it’s just you and me [inaudible].

RUSS MUNDY: I think so.

BRAD VERD: Patrik.

RUSS MUNDY: Oh, Patrik is an overlap now. Yes. Okay.

BRAD VERD: [inaudible] not to trust.

RUSS MUNDY: In the interest of time, I'd love to just immediately jump to the agenda, but we had something come up in the RSSAC meeting that just ended, or just after the meeting that ended, and that is the RSSAC chairs were approached by a member of the UN Global Commission on Security of Cyberspace, and they want to get input from RSSAC and SSAC in some of their work.

So my request of the RSSAC co-chairs was when they hear from and get the e-mail, and it was Wolfgang – I can't remember how to say his last name.

SUZANNE WOOLF: Kleinwaechter.

BRAD VERD: Kleinwaechter.

RUSS MUNDY: Yeah, that's him. Make sure that the SSAC chair and co-chair also get it, and we'll just coordinate things. But expect to hear something. We don't know what for sure. Brad, did you want to add anything, or Fred?

BRAD VERD: Yeah, I think he said he was talking to people in SSAC. I don't know who, but my comment to Russ was that if that's happening, let's make sure we're in alignment with whatever's being said and heard so that there's … And yeah, we had a conversation – we, the admin committee and a couple of SSAC members, because they had limited space, had a meeting with them the other night. So I don't know. There will be an ask of some sort, and being consistent when it comes to any response regarding the core of the Internet infrastructure, that might be helpful.

RUSS MUNDY: Yeah. Okay. Well, that was the only added item that I had for bringing up here, and so let's just dive right into our agenda. And it actually begins, the overview slide, and next, Mario, I think we go right to the RSSAC work plan, whichever of you gents want to describe that.

BRAD VERD: Oh, this is the organizational review, right? I'm sorry, am I looking –

RUSS MUNDY: Well, the workplan and for the coming year.

BRAD VERD: I got it. So yeah, I would say the topic that came out of the organizational review for us was to come up with a work plan, which quite honestly, we had already had on our agenda. We are working through that now. We believe we've identified a work plan, and we will be sharing it. I'm looking at Mario because – there's Steve. Somebody, Steve, can you guys help me? We're sharing it – we're voting on it, correct, soon?

So yeah, we have a work plan that's been shared with the group. We have a formal meeting tomorrow. RSSAC has our monthly formal meeting and we have it here so it's with the community should they want to participate, and we'll be voting on the work plan tomorrow and it'll be made public. It's really – how do I say it? It's not earth-shattering, but it shows kind of what our goals are for the year.

This year, it's a little odd because we're getting the work plan out, we're already through into the end of Q1. But going forward, this will be kind of our work plan that is done at the beginning of the year. It’s not something that kind of gets updated throughout the year, it kind of shows the plan for the year and the budget process.

RUSS MUNDY: Any questions on the work plan for RSSAC? I don't know that RSSAC has actually published one before. Have You? I don’t think.

BRAD VERD: No, we've never published a work plan, so this is new for us. Again, this is part of the review, and we've had our meetings with the OEC. We've given our feedback, we’re waiting for whatever recommendations are coming from the board. We’re kind of in a holding pattern with the OEC. But as I said, these were things that were already on our agenda, so we’re executing to this, even though it is a recommendation, we’re going to have it done.

RUSS MUNDY: Okay, good. Any questions from anybody on that, on the work plan? Well then I guess the next thing is the real description of what's going on in the work plan, is the review of the RSSAC work parties.

BRAD VERD: Do we have the work plan? Can we share it?

RUSS MUNDY: It’s in the slides.

BRAD VERD: Is it?

UNIDENTIFIED MALE: [inaudible] work plan.

RUSS MUNDY: Oh, yeah.

BRAD VERD: Alright. Yeah, if you can just provide the link in the chat, that’s all that’s necessary. So the current work, we have three open work parties right now. One is service coverage of the root server system. This has been ongoing for a bit. We've had – how do I say – less than stellar interest. Is that fair to say? Liman?

Liman is our shepherd from RSSAC to the work party, and there's really just not much engagement. Though this was listed as a priority from the caucus in a survey we did, we’re not getting much traction and much input on this. So we're kind of making a last-ditch effort right now to the group asking for input, to try to move the ball forward, and if it doesn't, then unfortunately, this will probably get shelved until there's further interest.

UNIDENTIFIED MALE: I'm just curious, is the lack of interest because people don't think it's a problem, or for some other reason?

BRAD VERD: There's a big sigh that just came out.

UNIDENTIFIED MALE: [inaudible].

BRAD VERD: I think – how do I say this – we, RSSAC has struggled with engagement from the caucus for a long time, and a lot of people want to be in the caucus, a lot of people want to listen to what's happening, but when there's one or two contributors, it makes getting stuff done really hard. So that's the challenge we've had. I think that's what this is suffering from.

When I get to the other work parties – there are two others. One of the two others that I haven't yet gone over, to me, is a higher priority, and to me, I want to focus my energy on.

RUSS MUNDY: So as a person who sits in both of these, the SSAC and the RSSAC, this particular piece of work, I see parallels in SSAC where there are people who will raise an issue, a topic of interest, that this is something that should be done, but when it comes to actually doing the hard work to get all of the pieces together and do the work, there's just not that many people that are willing to contribute.

So I think it’s a common – I won't say common, a similar problem to what SSAC has. Okay, Next, Brad.

BRAD VERD: Alright, next slide. I can't see the title, sorry. So service coverage, this is –

RUSS MUNDY: It’s the modern resolver.

BRAD VERD: I'm sorry, the modern resolver study. So this is the resolver study that is happening. This actually has a bunch of traction. There is work going on. We just got an update from Paul Hoffman in our last RSSAC meeting. So there is work underway, they're creating a number of tests in a lab, and they're trying to make sure that those tests are repeatable so somebody else can go out and do them. So there is progress being made here.

We obviously don't have a final product yet, don't have a date for it, but work is underway and happening. Is there anybody else who wants to add to that? I don't know who the shepherd is for that off the top of my head.

RUSS MUNDY: Paul's back there.

BRAD VERD: Oh, I think it's Fred. Anything you want to add?

FRED BAKER: Not really.

BRAD VERD: Any questions? Alright, let's get to the good one. Next slide, please. Yeah, okay. So this is the work party that we just started, this is the root server metrics. This is where I think – well, let's just say the chairs of this work party are Duane Wessels and Russ Mundy.

I'll speak on my interpretation on what the goal of this is. This is to define what “good” looks like for the root server system and the root server operator. So this is something that has been attempted a couple of times throughout history. This is going to try to put some very specific metrics down that should cause interesting discussions.

We've had our initial phone call with the work party. We have about 20 members so far. I continue to encourage everybody in RSSAC and the caucus to engage and be part of this, because this is going to be impactful. This could dictate changes to root server operators and the root server system.

We had an open work party here yesterday, or the day before yesterday in this room made some progress. We've created a calendar of work going forward, we have a number of phone calls. There is a workshop that has been scheduled in Virginia, and so this is lots of work going on here, lots of engagement here.

Myself and Wes Hardaker are the shepherds of this work party. While I don’t have dates to give you on outputs, and I think I want to be careful or be cautious to provide when we will have an output, because as I said, there's going to be some passionate discussions and work done in this work party, and I think the goal here would be to do it right rather than to do it fast. That’s my thought that I've been sharing with the group. Wes, anything you want to add?

WES HARDAKER: No, other than this is a pretty important piece of work, and the more input we get for what the system really needs to look like, the better it will be. This is work that'll probably stay standing for quite a while, so if you have any interest or any thoughts on how we can best measure and ensure that the root server system is stable and secure, now is the time to give us that information.

BRAD VERD: Yeah. I think really quickly, I'm sorry, just to give a little bit more context, in my eyes, and how I've been kind of couching this, is this is the complimentary document to RSSAC 37. RSSAC 37 gives you a government accountability of the root server system. This document should give you the technical accountability to the root server system and the root server operators that either stands on its own should 37 not be implemented, or once 37 is implemented, this becomes the bar that is measured and worked against within that model.

SUZANNE WOOLF: Yeah. The word “correct” is interesting to me, because when I look at it from a security perspective, I'm always wondering, well, what can be spoofed? And so looking at, is there anything in there that covers integrity of answers. And I don't know how to word that exactly, but really, it’s not just about performance, but is, “Do you know that these are correct?” But being a little bit more explicit about what does “correct” actually mean.

LARS-JOHAN LIMAN: My interpretation of this is that the client receives DNS information that the root server administrator and maintainer puts into the system on their end. But if it’s not clear from the text, then some text should probably be polished somewhat.

UNIDENTIFIED MALE: Liman, I’d like to clarify something really quick, because there's a lot of infrastructure between what the root server system provides as an answer and what the client gets. So really, in my view, it’s the same thing, but it’s really the answer that leaves the root server system is correct, and then what happens beyond that is subject to many other boxes that we are out of control.

RUSS MUNDY: So I think we've got some very good points here, and I can say as one of the work party co-chairs, these are the kind of inputs that we want to have and these are the kind of discussions that have already started.

So, Jay.

JAY DALEY: So this is also something that I wanted to point out of the SSAC people. that should be a very nice step forward in answering an old and open SSAC question that SSAC asked ICANN and the board to do probably five or six years ago, measure the system as a whole.

I forget which of our advisories it’s in, but it’s in there, and we've asked that at least once, maybe twice.

BRAD VERD: Just really quick, a little bit more context, we wrote the statement of work kind of as open as possible, but we've instructed kind of given the work party the latitude to change it as needed. But we've kind of hinted that there's a couple different outputs that come from this.

Either it’s a brand new document, RSSAC document stating the service level expectations for the root server system and root servers, this could replace RSSAC 001 which is the current one. It could be an RFC if necessary. We could publish an RFC of what the metrics and measurements are. Or it could be both. It could be an RSSAC document and then the RFC is published, maybe not with the thresholds and specifics, but generic, "These are the metrics that are taken" type of thing. So all that is kind of put in the hands of the work party right now, and as I said, they've only had two meetings.

RUSS MUNDY: I think Daniel was first.

DANIEL MIGAULT: I'm going to be brief, but back to the initial question, security is a concern. I think clearly, yes, it's something that we will look carefully at.

UNIDENTIFIED MALE: I was going to observe, yeah, I think that given the current RFCs about more protocol capabilities and whatnot for expectation for root server operators, that seems like a good idea to me, especially in light of – well, I think this is stellar work, I think this is long overdue, and issues as recent as a couple of weeks ago when there was a prolonged root server outage, I think, aren't acceptable, and I think this is going to shine a light on that, and then we need to begin to address those things as a community as we mature this system, or people are going to find alternatives.

RUSS MUNDY: Okay. Any other comments or questions on the work parties, and in particular, the metrics? Okay, so I think then that gets to the next big item with RSSAC, and that's this review of the current state of RSSAC 37 and 38.

BRAD VERD: Alright. So 37, obviously, this is not the first time you've heard us talk about 37. This is ongoing work. When we turned this in to the board June of last year, we strongly encouraged, let's say, the board to not go off in a vacuum and create a response and hand it to us. So we encourage the back and forth kind of dialog to make sure that whatever the board was coming up with in their response was on the same trajectory that we were on with 37. So Kaveh, keep me honest here.

Cherine and the board has been very apologetic for not getting back to us, so for some reason, Theresa sense of urgency to get a response to us. But right now, what's happening – which I think is very productive – is the response to 37 has been turned over to the policy team within ICANN, to David Olive, and they have been working on a concept paper.

So they've come up with a concept paper which basically takes 37 to the next step on how to move forward with 37 in the community. And that, they have provided back to us on an informal basis, and we have gone back and forth with the BTC in editing that document, which is a bit schizophrenic because RSSAC is now editing a document that will be coming to RSSAC from the BTC.

But this is what we asked for. We asked for this type of dialog, this iterative approach, and I think everybody has been very pleased with it, very happy with it. We're all on the same page. We met with the BTC yesterday, they're all very pleased with our edits.

It doesn't mean that they're going to accept our edits or publish it, but they were very receptive to it yesterday. That's what's happening right now. Going forward, now that we've given our informal feedback to the BTC, they will take that and they have their own workshops and their own meetings. In theory, the timeline is right now that they would approve the concept paper in May, and at that time, it would be sent to the board, sent to RSSAC, and would go out for public comment and review at that time. Is that correct, Kaveh?

KAVEH RANJBAR: So after they approve, we made sure that there is a step. After hopefully May, the BTC approves the concept paper, they will send it first to RSSAC, and then RSSAC will have a chance to vote accept or not accept. Then if RSSAC accepts that document, it goes to board. If it doesn't, we don't know what happens, but I find that unlikely because we are working together.

BRAD VERD: Yeah, because we are working hand in hand. So at that time, when RSSAC formally gets it from the BTC – right now, we have not formally gotten it even though we've seen it and we've made edits to it – that is when the liaisons could take it. So Russ could take it, share it with SSAC, Daniel could take it, share it with the IAB, and then there'll be some vote on it within RSSAC to approve it. At that point in time, the BTC would give it to the board, and then that begins the process. So that's where we stand. Any questions?

I think we're looking at – is it Marrakech, potentially, for a board resolution on it?

RUSS MUNDY: So in terms of the SSAC processing of it in terms of SSAC needing to pitch in formally, it'll be after the June meeting probably, if that makes sense.

BRAD VERD: Yeah, I would certainly want SSAC's input as we start to work through it. The concept paper creates basically a governance working group, and the working group is comprised of the stakeholders that are identified in 37, which include the IAB, the root server operators, and the ICANN community.

So there's a group created, and then they essentially take the inputs, which are RSSAC 37, the concept paper and the public feedback, to finalize a model. They would finalize the model based upon some timeline that we don't know what that is yet. They'd work with the community, we'd work with SSAC. We'd work with everybody to kind of finalize what the model looks for.

They would come up with the final model, and then the next phase after approval from the stakeholders would be the implementation of that model.

ROD RASMUSSEN: So I see two potential touchpoints for SSAC there, one being this committee, whatever, the stakeholder group. Would that be something that – I'm pretty sure the answer would be yes, that you'd be looking for SSAC to, SSAC members at least to participate in potentially. And then what would the rules of engagement be there? Because there's obviously overlap.

And then the second area is – and this has been discussed for like a year now as a potential for SSAC to more formally put in. obviously, we've gotten feedback from individual members over the course of this. We need to just know if there's going to be some sort of –and I'm just asking this, I know we've already had an offline conversation – if there's a formal ask for us to comment on whatever this thing ends up being that comes from the board, BTC or whoever, that we can anticipate that so that we can work it into our schedule.

BRAD VERD: I think that formal ask would come from the resolution. Correct, Kaveh? Whenever the resolution, we're speculating right now Marrakech, that's when – or no. I'm sorry. Yeah, speculate Marrakech, and then it would go out for public comment. At that point, we would certainly ask for the SSAC to comment on it.

RUSS MUNDY: And in response to your other question, Rod, about SSAC participation, although this whole structure that's being put in place is [one's] being created. So there's not that many models.

But in some ways, there are parallels to what was done in the IANA transition. So I would see that for instance there would be a role for SSAC on one or two of the committees, like the government committee already lists SSAC as a member. So it would be like providing a member to the CSC.

So yes, another external tasking for participation from SSAC.

BRAD VERD: Yeah. Really quickly, I think we've learned as we go through this that this is a bit of green field work here in the sense that the policy work that's being done here within 37 doesn't fit into the normal ICANN policy work. So we're kind of having some growing pains, which is why it's been nine months since the board kind of has responded. And that's okay, we're figuring it out, we're working through it. But this is green field, so at any point, we want input from groups to help guide this and make it right. Because again, the goal is to do it right, not fast.

RUSS MUNDY: Kaveh.

KAVEH RANJBAR: A quick comment to continue what Brad said. Yes, it's basically a green field project, but one of the things that we both have mentioned also yesterday in BTC, but both board and actually want maximum inclusion, because this is something that will basically govern the chunk of how Internet works, which his much bigger than ICANN. And for this to be sustainable, we really want something that everybody who has a say at least had a fair chance to be able to participate. So definitely, SSAC is one of those groups, because we want to make sure that not only when the work is done, but in 10 years or 15 years after the work, if someone questions, "Hey, why this is like that?" We can show we have done our due diligence and included anybody who had a say in this. So that's the guiding principle for all of us.

RUSS MUNDY: Okay. Thank you for that good discussion. Any more comments or questions on the state of RSSAC 37, 38? Go ahead.

BRAD VERD: Again, going back to – adding to what Kaveh just said is this diagram that's up here that you guys, I think, are pretty familiar with. This is the evolution of your diagram that came from an SSAC document years ago.

UNIDENTIFIED MALE: [inaudible].

BRAD VERD: But what you see on the left in the white box is the governance that was kind of covered in the transition, and the blue box on the right, which there is no governance, is what we're trying to do on 37. And the whole together is kind of the full ecosystem. So you can kind of see what's lacking. Okay?

RUSS MUNDY: Okay, so that's the end of sort of the RSSAC-specific part of the agenda, and now we move on to the SSAC portion. I will, for that, turn to Rod to ask him to either take it himself or pass it to appropriate people to comment on. Just to review the current work, right?

ROD RASMUSSEN: Okay, I'll run through. I've got so many decks that I've looked at recently, I don't remember which slides are on this. So we'll see as we go.

This is just a quick overview. Do the slides contain any more details on any of these projects, Russ?

RUSS MUNDY: A little bit. The next one does, but that's it.

ROD RASMUSSEN: Yeah, a little bit. Okay. So NCAP is one that I'm sure you've heard about, at least I hope so. There is a board resolution that is pending for Thursday. All signs point to "yes" for launching what was the first study around bringing in the data, the definition of name collision, understanding the scope and scale of the issues in the current state versus where we were ten years ago or what have you when we were looking at this before.

RUSS MUNDY: There are several slides on NCAP later.

ROD RASMUSSEN: Okay, there are several slides. So we will get down to that. I'll just do this very quickly then. Organizational review, we're going through the final phases. We have a mid-June deadline for a formal response, but we're incorporating all that stuff which ties into some of the work we're doing internally on our own processes.

We have an IoT thing coming out. Do we have a slide on that later?

RUSS MUNDY: No.

ROD RASMUSSEN: No, okay. So Cristian Hesselman has been leading the charge on that, and that's going to be kind of defining the risk space, opportunities, etc. within the DNS world. So we're looking forward to getting that out shortly. We were hoping to get it done by here, but it's almost done. Right, Cristian? Yeah. We have a work party meeting on that over lunch.

I've already mentioned working on our own processes. Merging security topics, we're doing this as a standing thing at tech day. For those of you who were there yesterday, you saw us talking about DNS hijacking or domain name hijacking.

RUSS MUNDY: There's a few slides.

ROD RASMUSSEN: There's a few slides about that. Okay, I'll get into that. DNSSEC workshops, obviously that's tomorrow. It's still our official mantra, and there's some interesting stuff going on in the background about making sure that's going forward. I don't know how that gets budgeted and things like that, but we fully intend that those will continue to go without us interfering at all.

So on membership, actually, I'm making this appeal in various places. We are definitely looking – so we have an annual membership process where we're bringing in new members, and we have the same challenge a lot of people in ICANN do, is bringing in people from various backgrounds. With us, technical, security backgrounds are most important, diversity there, so that's always something we're looking for first, but we also are looking for more geographic diversity and the standard ICANN diversity request.

But in our case, the geographic is particularly interesting as far as different operational environments. So like myself and many other members of SSAC live in North America or Europe or what have you. We have very interesting problems that are very large-scale and we have very good bandwidth to deal with, which creates its own problems, but other people from other parts of the world where the bandwidth itself is questionable, we don't have very good representation of that, and they have different kinds of problems that they deal with. One of those things you had on your list was probably related to that.

So anyway, I want to make sure that if you know some folks in those parts of the world that have good security chops and operational experience, please send them our way to apply, because we would really like to expand our capabilities there. And I know folks in this room have people out there they know. It doesn't have to be a person who comes to ICANN meetings all the time either.

And then just as a, "Yay, we finally got something done on this," which has been sitting around for a while, is the EPSRP, which is – Patrik, what's EPSRP stand for?

It's the thing that ended up being all about Greece – string similarity, and it was a lot about Greek and dot-EU version, and Greek characters ended up being the driving force there. The ccNSO sent a letter and some other correspondence last week that hopefully will get that off the table. Uh oh, is there something new, Patrik?

PATRIK FALSTROM: Well, I need to know how to Google, still. Extended Process Similarity Review Panel.

ROD RASMUSSEN: Yeah. So we just called it EPSRT because we had no idea what the actual –

BRAD VERD: I'm never going to remember that.

ROD RASMUSSEN: And hopefully it will never come up again. Okay, want to move on?

RUSS MUNDY: Yeah, new topics.

ROD RASMUSSEN: Okay. [inaudible] new work, right? Next slide, please. There we go. Yeah, so here are areas that we're looking at. This is pretty much the same list as last time, except there's one interesting new one on there. We're actually trying to tin bash some sort of charter around the [inaudible] DPRIVE, and now the DOC, DNS over Cloud. I've heard that term now, which is kind the browser talking directly to the CDN network issue, or the application talking through some nonstandard way to a resolver that's residing in a nonstandard DNS resolver space, looking at that. So we'll see if we're going to get that off the ground. We have a lot of interest in the membership to talk about this, but we have to figure out exactly what we want to talk about and what we may want to say.

That second topic there is on our list and might be of interest at some point for you guys.

BRAD VERD: I think both the first two topics are interesting. The first one obviously has a direct on root server system, and the performance, really the capacity as we talk TCP. And then I know we've talked about pros and cons of the hyper local root, and we'd love to be engaged on that.

ROD RASMUSSEN: Yeah, and definitely, if you or other RSSAC members have input on the first, that's great, because as I said, we're trying to form that. We're in the forming stage in that work party. And then obviously, if we're doing hyperlocal root, we'd be having Russ engage to see if there was some interest in perhaps doing some [inaudible] work there.

The DS key management, this gets into some of the things – you've got multiple providers for your DNS services or you're changing providers and how you manage that without losing your signing or integrity signing over that transition, or just being able to operate with multiple providers, those are some challenges there.

Takedowns, that's takedowns of domains and various other things on the Internet. That's been one of those, looking at abuse in the new gTLDs and understanding the whys, wherefors, and what driving factors might be able to drive that down, metrics probably as well.

The new one is the hijackings, taking a look- we've said a lot about this stuff before in [hygiene,] registrant protection, registrar safeguards, things like that. So we've got a boatload of documents on that. But the recent things that have been going on, we may take another look at this, especially since the sophistication there – do we have slides on that one, by the way?

RUSS MUNDY: That’s either John Crain or David Conrad will be giving us a few words at the end, no slides.

ROD RASMUSSEN: Okay, yeah. This is something that everybody in the ecosystem really needs to be aware of. We had a conversation last night where some of the ccTLD operators are not even aware that this is going on, and they were the ones most affected. This, we really need to raise the priority and the visibility of what's happening here, because the sophistication of these attacks and how they're going after us and infrastructure is really important. So how can we as a community that are clued up on this raise that awareness and make sure that people are monitoring, protecting and mitigating?

And then of course, what we just talked about, responding on 37, 38, whatever the model is. Okay, next slide. Any questions on that before we dive into any of those? Any questions on those topics?

RUSS MUNDY: Daniel.

DANIEL MIGAULT: I just have a question regarding the DS management. So what is actually the real problem? Is that you sign my zone and I want to change the provider, so how do you –

ROD RASMUSSEN: Transition that.

DANIEL MIGAULT: Okay. And what approach you're trying to do to solve that? Is that to split the signing?

ROD RASMUSSEN: So the work party would actually look at the problem and come up with some potential solutions and recommendations around that. This is something that's been kind of kicking around, and it's fairly specialized. There's only so many people doing this kind of thing. But also, for people who are trying to multihome their authoritative DNS, it's actually a current operational issue potentially. And I know there's some IETF kind of work going on here. Even though I'm not an IETF guy, I hear things. And there's a few folks that have been looking at this particular problem.

That’s why it came to our radar. I think Steve Crocker actually brought this up as an area of concern that he's had for a while.

DANIEL MIGAULT: Okay, so in IETF DNSOP?

ROD RASMUSSEN: Yeah. [inaudible].

DANIEL MIGAULT: Oh, DPRIVE.

ROD RASMUSSEN: Yeah.

DANIEL MIGAULT: Because I know that similar approach has been – not similar, because I don't know the problem, but we also had this signing – splitting TLS between a cryptographic service and the other things. So that might be –

ROD RASMUSSEN: That might be actually of interest to add to that as well, because I'm trying to get a bucket of those kinds of things to actually talk about.

DANIEL MIGAULT: Okay.

ROD RASMUSSEN: Because it all ends up getting back into this how do you do this coordination and the like. So if we're going to be talking about those control plan issues, let's do it all in one group.

RUSS MUNDY: So, any more questions on the potential future work portion for SSAC? No? David.

UNIDENTIFIED MALE: Hello. Had to wait for the mic to boot. There we go. Just a though that I'd had. The DNSSEC workshop on Wednesdays, I guess, would it [inaudible] to maybe evolve that into security for the DNS ecosystem to move to a – especially in light of the DNS hijacking attacks? Do I need to repeat that?

ROD RASMUSSEN: It was on the mic.

UNIDENTIFIED MALE: Okay, so I'll just repeat it. In light of the recent DNS hijacking-related stuff, would it make sense to evolve the DNSSEC workshop to focus more on DNS ecosystem security instead of specifically DNSSEC?

RUSS MUNDY: Well, I'm glad you asked that question, David, because that is in fact where we've been migrating to very quietly and subtly without doing any name change at this point, but in fact that's kind of where we've been heading, because if you look at the agendas over the last three to four meetings, you can see some of the ties to DNSSEC are only very loose, so we're definitely heading in that direction.

One of the reasons we've not discussed changing the name is purely political at this point, waiting to see when the right time is to actually change to doing that.

ROD RASMUSSEN: Yeah, in December we were doing some strategizing about exactly that. Did you plant that question?

RUSS MUNDY: No.

ROD RASMUSSEN: Okay. John.

JOHN CRAIN: You may not be aware, but within OCTO, we've been doing some work studying DNS abuse, etc. And also –

UNIDENTIFIED MALE: Really?

JOHN CRAIN: Yeah, just a little bit. And operationally, we've been involved in some of the takedown work and trying to understand that. So love to see you guys working on this stuff, and if you need input on what we're doing, more than happy.

ROD RASMUSSEN: One thing we may be coming to you for is potentially data that you have that may not be publicly available.

JOHN CRAIN: Yeah, please give us a very clear description, because I'm going to have to go to Legal. If I could share everything I had, I would.

UNIDENTIFIED MALE: We don't want you to, so –

JOHN CRAIN: Yeah.

RUSS MUNDY: Okay, any other – yeah, John.

JOHN CRAIN: And just to give a shout out, because I want to embarrass her and people are probably wondering who walked into the room. Samaneh – if you'd like to just wave quickly – is our new researcher and SSR specialist, and she's working on the abuse stuff. So no pressure.

RUSS MUNDY: Okay. If there's no more questions or comments on – did you have something, Brad?

BRAD VERD: No.

RUSS MUNDY: No. Okay. Paul Hoffman is going to lead our discussion. In fact, there's a chair at the table. Why don't we –

PAUL HOFFMAN: I'll spoil it for you. So we were requested to talk about a few things that are from OCTO about KSK and such like that, so we've got a couple slides here. Since I don't normally sit in these meetings, I was told in the last RSSAC-meeting you were brought up to date about the rollover, but that was soon after the rollover. So what happened since then?

Actually, between then and January, almost nothing happened. That is we kept thinking we were going to hear more problems with the rollover, and there were really an exceptionally small number given that on any given day, part of the DNS is on fire anyways.

On 11th January, we revoked KSK 2010, and for those of you who aren't into the depths of modern DNSSEC, that actually means we kept publishing it but with its revoked bit turned on. So we didn't expect any problems with that because it was already in there. This was literally a change of one bit. And as you'll see in the next slide, we were wrong.

Before I go to the next slide though, I just want to say we have one more visible change happening, which is on the 22nd of this month, which is that record is going to be pulled out. And we don't expect any problems. Next slide, please.

So you'll notice that the green line stats on the left and doesn't stay horizontal or go down, as one would have hoped. So when we rolled the key, the number of DNS queries going to the root jumped, and we excepted a little bit of that, and we also expected it during those two little red bars on the left, meaning as it’s happening, people would say, “Oh my god, my system’s on fire,” and shut it off or fix it.

You'll notice that after that, it actually went up and then stayed stable. What that means is there are a whole bunch of systems out there that after we rolled the KSK, they're doing something insane and they are hitting the root servers quite often.

Second set of vertical bars where it says “revoke,” where we didn't expect any problems, you'll notice that that jump is actually bigger than the first jump. And we have some theories why, but the summary is there is bad crap out there in the resolvers, and those resolvers are not being monitored. That is, we believe all of the resolvers that are the diff between the first line and the second line and the diff between the second line and the third line are resolvers that most likely have zero people or zero systems relying on them, because it is extremely likely, sort of if you think about it, that all of those are giving serve fail for every query. They think they're doing DNSSEC validation, and for some reason, they aren't. But no one knows it.

So I'm hoping we don’t have another parallel set of lines like that on 22nd of March. I'm predicting that we don’t, and I've been wrong before. Actually, let me stop here. Any questions on this just on what has happened since the rollover?

FRED BAKER: So, is that the discussion of AS2510, or is that a separate –

PAUL HOFFMAN: I'm not sure what AS2510 is.

FRED BAKER: AS2510 is sending in a whole lot of requests for the key.

PAUL HOFFMAN: That's one of the ASes. There are a bazillion of them. This is at least 10,000 systems, we believe, spread across the root server operators.

UNIDENTIFIED MALE: Yeah, so I have a presentation tomorrow in the DNS workshop which confirms this as well.

PAUL HOFFMAN: Okay.

UNIDENTIFIED MALE: We saw recently another significant increase. So at A and J, we're seeing a billion DNS key queries a day right now.

PAUL HOFFMAN: Okay.

UNIDENTIFIED MALE: And it continues to go up.

PAUL HOFFMAN: And has that increase been from a small number of IP addresses, or many? Or have you not –

UNIDENTIFIED MALE: Many IP addresses.

PAUL HOFFMAN: Okay, right. Yeah.

UNIDENTIFIED MALE: Yeah. Maybe a small number of ASes, but many IP addresses.

PAUL HOFFMAN: Yeah.

UNIDENTIFIED MALE: So I'll present that tomorrow.

PAUL HOFFMAN: Okay.

DUANE WESSELS: Maybe it would be useful to say there is outreach happening related to this, as you probably know. Obviously, we want to get to the root of what's going on.

PAUL HOFFMAN: Well, and we did outreach after the first one as well and got no response at all. So that's one of the reasons why we informally think these are systems possibly with no operator running the system either.

DUANE WESSELS: But I think outreach to closure, not just outreach to ignore a billion queries a day. Because if these things are going to be persistent and somebody is going to address it, then either reach the ISP or the upstream until we resolve what the issue is, not just an e-mail and let it go.

PAUL HOFFMAN: Okay. Well, yeah, no, we weren't doing just an e-mail and let it go either, we just weren't getting any response to any of our outreach. If you have any luck with that, we would love to hear how you had luck with that, because then we can do it for others.

UNIDENTIFIED MALE: [inaudible].

BRAD VERD: Yeah, I think this is a new jump in traffic, so above and beyond the bar [inaudible].

PAUL HOFFMAN: Yeah. Right. I got that.

BRAD VERD: And it's a significant jump. It's not just a little, it's a significant jump. So Duane found it in A and J, we've confirmed with other root operators that they're all seeing it. we've confirmed ASes that ASes are all similar. So there's going to be some outreach to these people to try to figure out what's going on and what changed, because it dramatically changed.

PAUL HOFFMAN: Yeah. And this could be happening again later.

KAVEH RANJBAR: Just to confirm what Brad said, at K, we had on average 600 DNS key queries per second. After that revocation, it basically jumped up to 8000 queries per second. So from 600 to 8000 basically after one event, and now it’s consistently at that rate, growing slowly, not exponentially [inaudible].

PAUL HOFFMAN: Right. And my personal theory on the growing slowly is that there are systems that are configured in a certain way that causes the jump, and those are now being actually turned on. What we've been seeing in the past was a certain way, and some systems that have a new configuration are simply being turned on, and so they immediately go into this mode.

We certainly have not been hearing anything from anybody saying we’re seeing validation problems or this ISP is going down or whatever. So this is all hitting the root server. Any other questions on this, on the rollover so far? Okay, next slide.

So given that data and lots of other opinions and such like that, there's question of, well, what should we do with the KSK in the future? What have we learned? And there is a mailing list that we actually had set up last year, and there's discussion on that mailing list.

We greatly encourage people who have an opinion about how the KSK should be handled in the future, number of KSKs, backup keys or standby keys, any of that, to join the mailing list. And we've been pushing that. So far, there's been some discussion, but not as much as, say, a typical flame war in the IETF yet.

But we’re also about to have three face-to-face meetings, and at the face-to-face meetings which I'm running, we will be emphasizing it’s fine to stand up at the mic now, but really, go to the mailing list, because saying something at the mic lets you say something, saying something on the mailing list lets people respond and to work it through. So next slide.

So the three face-to-face meetings are tomorrow here as part of the DNSSEC workshop. We’re going to have another one in a couple weeks in Prague. Thank you, Warren, for turning that into an actual [inaudible]. It’s not a side meeting. So we had two informal face-to-face meetings at the last IETFs that were side meetings, and they were reasonably well-attended as random side meetings. Particularly one of them was on Friday. So this one’s going to be a real [inaudible], so it’s on the agenda and such like that. And then a third meeting at the DNS summit in

Bangkok which is ICANN’s technical DNS workshop. It's two days which are immediately before DNS OARC. And it’s immediately after the GDD summit. So I don't know how those two [roles] will collide correctly.

UNIDENTIFIED MALE: [inaudible].

PAUL HOFFMAN: Well, yeah, and that actually happened when we did this last year, that a bunch of GDD people who were sort of interested in operations actually stayed all the way through OARC. So that was nice.

So after those meetings, the mailing list will continue to be open, but the next step after that is – this is IANA’s job. IANA is in charge of this, so they’ll be looking at the mailing list, they'll be listening to the conversations, and this is informal, but probably by the end of this year, they will say, “Here's what we heard, here's what we heard that is doable,” and they will propose a plan. And that’ll probably go out to public consultation. However that goes. Not clear, but that’s how we will go from here. Any questions on this? So we hope to see you, some of you at least if you feel like – oh, sorry. Tomorrow, or at the other ones, but certainly, what we would definitely like to see is interaction on the mailing list, because that's the best way for IANA to get the input, not just hearing that a person said something, but a person said something and either no one objected or a couple people did plus ones and such like that. Okay. Thank you. I think that was my last slide. Yeah.

RUSS MUNDY: Yeah. Thanks very much, Paul. So next, we'll move on to the status of the NCAP project. So, Rod?

ROD RASMUSSEN: Yeah. Can I have either Jay or Jim? I don't know who's in the room [at the moment.]

UNIDENTIFIED MALE: [inaudible].

ROD RASMUSSEN: Oh, okay. You want to run through that? Okay, there's Jim. Didn't see you back there. Jay can do it.

JAY DALEY: So we did some work through a work party to define what we mean by name collision. So you can see here some of the things we've done so far. Sorry, I'll start again. This is what the board has asked us to do. it’s a very detailed request form the board. It’s far more detailed than anything we've ever had before from SSAC.

As you can see, it’s specifically looking at collision strings, and it’s also looking at corp, home and mail. So it has a direct impact on future rounds of new gTLDs being delegated. Next slide.

Right, so within SSAC and within the work party, we produced a project plan. That went out to public comment, and we had really quite some thorough public comment on that. Much of the public comment was about tying the timetable to which we’re working on NCAP to the next round, or not tying it to the next round. There are people very concerned that this is going to slow down the next round of new applications, and our response to that was quite clear, that that’s a board decision, all we’re doing is offering advice on this.

We then did a – sorry?

ROD RASMUSSEN: Just want to clarify there are some that think that’s a bug and some that think that’s a feature.

JAY DALEY: Absolutely. So we produced a revised project plan, but when we produced the revised project plan, it became very clear to us that this is not really the same as any previous SSAC work party. With such a detailed board request from us, we have a fixed timetable we expect to deliver it to. There's a fixed cost, a quite large cost, in the millions, and extensive use of external contractors.

This is not the same as just a group of people that have a discussion and produce a report at the end of it, it's a formal project. So we want back to the ICANN board and said, "Right, we believe this is a formal project and should be run by ICANN as a formal project with us providing advice to that formal project." So that was agreed, and OCTO was chosen by the board to run that formal project.

OCTO then have looked at the project plan, and they have made one change. Next slide, please. It's not on here, but OCTO have made one change to that, one substantive change, which is to put less into the first of the three studies, which will slightly lengthen the term of the project but is better at giving OCTO a clear endpoint for study one and a yes/no, stop/go point for the rest of the project.

So we're just waiting for the board to officially sign that off, the new OCTO proposal, and then we're going to move into the administrative side of things with the work party which is setting up the mailing list, doing the statements of interest and those things, and potentially appointing a third co-chair to work with Jim and I, who would be somebody outside of SSAC. And then we'll then begin work on study one, which is the review of the previous work, and that's where we will be gathering our thoughts on what that means, working with OCTO to produce a statement of work, and OCTO simultaneously – or probably simultaneously – be working on an RFP process for external contractors who can deliver these type of things. So we're hoping that should start at some point soon after a very lengthy time of planning it. Any questions at all?

RUSS MUNDY: Okay, great. Thanks very much, Jay. No questions from anybody on this? Okay, good. Now everybody's up to date on what NCAP is doing. Next item is recent domain registration hijacking, and it's a shortened derivative presentation of what was done at tech day, and I think Rod is going to do that.

ROD RASMUSSEN: Yeah, I think it's just one slide, and then there's a special briefing from OCTO as [inaudible] follows that. So, how many folks in the room here are not familiar with the attacks that went on? Okay. Yeah, right. Is anybody not familiar with the attack stuff that happened with various middle eastern government agencies, etc.?

BRAD VERD: Yeah, I believe RSSAC is familiar, and the RSOs are working on a joint statement.

ROD RASMUSSEN: I don't need to waste time on this then, because we should just get down to brass tacks about talking about what's going on. We have at least one really directly affected person in the room. Looking at you, Patrick. And then others that have been working really hard on the various issues that came up. This has actually been a really good nexus point for bringing people together to talk about these things. This is a good room to have a little bit more discussion on that. So I think we can just go over to what OCTO – I think the next slide here is the OCTO presentation, if I remember right.

JAY DALEY: Okay, well, we do have a slide set that we're not going to show, but Russ, feel free to distribute them, that we've been using to update the board and others. So I'll talk a bit more about our view on this and what we saw rather than the technical elements, because I think most people are familiar with those.

So life is full of irony. So as I sit there thinking about how we could maybe do some kind of exercise for the ecosystem and maybe do some kind of tabletop or something which is a project on my list of thinking about how we exercise emergency processes and things, we receive in the IANA requests for an emergency change to a ccTLD with the indication that it's due to a breach.

So obviously, the IANA does that. there are various communications between ICANN, Verisign, etc. At the same time, I received telephone calls from some of the affected parties saying, "Hey, this is going on."

And then you sit there and you think, "Okay, how are we going to communicate with all these people?" So what we understood after being read in and by looking at some of our data, that we're talking about 12 TLDs, CCs and variants of different scripts. Remember the round where the ccTLDs got their country code in other scripts. A couple of those that were associated with the same TLDs, mainly in the middle east but not solely.

We don't know why. In fact, the first one that came in was not in the middle east, it was from Asia. So what we did is – and by the way, we had communications with all of those TLDs about making changes, but only a couple of them said, "This is an emergency change, we've had a breach." Most of them just made changes.

So what we do in ICANN in this kind of situation is we form what we call our emergency response team, our emergency management team which consists of various groups within the organization. Of course, we need lawyers because you can't have any kind of team without lawyers, communications people, etc. Any of you have crisis management teams, the standard sort of process.

And we kind of had three phases. One is understand, so try and get as much intel as we could so that we actually understood what was going on. And I will say that even those people that are directly involved, I don't think anybody with 100% surety understands really exactly – it's the fog of war – probably not the best word to use there, "war," but it's the fog of the moment and you don't necessarily know.

So what we first did for our CMT, our crisis management team, is try to figure out what was fact, what was hearsay, and what was just people making stuff up.

It turns out that most of the press reports are relatively accurate. I don't think any of them are exactly precise, but most of them from their viewpoint were pretty good from what we've learned from bot the reporting parties and people involved.

So that was a big part of it, find out what's going on. And then you need to decide what you're going to do. So there were two kind of approaches for us at ICANN. One was, how do we ensure that the affected parties are informed so that they can take action after we've learned about this? And we worked with the reporting individuals, the people who were sharing data with us, and affected parties to make sure that they could actually communicate and share data.

There was at least one contracted party, a registrar who was affected. They found the mechanism for access, the vulnerability that was affected. It was not a DNS vulnerability, it was something else. Did repairs and looked at their systems, etc.

We drafted a response that mainly pointed people to the things that were out there in public, so most of the information that we received, both David and I, from the trusted communities, was TLD red, traffic light protocol red. So we couldn't just go out and share it with everybody. But there was enough information out in the public that we could point people towards those.

So we reached out to all the contracted parties, because obviously, we have security contracts for all of those. And we reached out via the [trust] group that ccTLD security folks have, and operators, and pointed them towards the events that were occurring. And we did some individual reach out when we knew that somebody was specifically affected.

And then the other thing that we did is we made out a couple of public announcements, which I think – and I've been at ICANN a long time – is pretty much unprecedented for us to go out and say, “Hey, guys, go look at this as an issue.”

I think everybody in this room knows that, yes, they were complex attacks in sort of the breadth and the organization of making the attacks, but the attack vectors were – yeah, they weren’t that sophisticated.

So we've wound down the crisis management team for now. We've communicated with everybody we do not believe the attacks have stopped. In fact, we’re pretty sure this is going to continue at some level. It’s purported to be nation state. Everybody in this room knows that attribution is hard, and ICANN has no opinion on that, who it was. But it was certainly a sophisticated actor. They understood things about how the DNS ecosystem works that was surprising. They’d done their homework, understanding when zones refresh and things like that.

UNIDENTIFIED MALE: [And timing.]

JAY DALEY: Yes, that's what I mean. They were very good at timing. And this is not something that just happened. If you've read the reports, you'll realize that this has been going on for at least a year that has been found out about.

So I think in summation, this is scary. When you get sophisticated actors like actually planning this out and doing this, everybody in this room knows, of course, that if you take away the parent, if you can actually compromise your parent zones, the people above you, then you can be in a lot of hurt.

So we have a session here on this in the security workshop. There were sessions on this, so people are talking about it. In our briefs that we put out, we pointed people towards the long-existing SSAC advice, multiple documents on this. We did a little list of all the basic things that people should probably be doing anyway.

And now I think we as a community – and of course, ICANN staff – have to figure out how we're going to raise the awareness so that people in the industry at least have a better understanding that, yes, we really are vulnerable.

It was a pretty long week or two, but I went on vacation, so I was doing most of this from poolside. So it wasn't completely terrible. But it was a bad week. And I think we're going to be looking to SSAC to help us pull the advice together and then figure out how we can help promote that. and Merike's been helping with this as SSAC liaison to the board. And I think we're going to be busy. Cris.

CRISTIAN HESSELMAN: So you mentioned that a lot of the data you've gotten is TLP red, but obviously, there's a lot of other stuff that's percolated out into the world through various means. Do we have sort of a set of talking points for other industries and such that we can talk to about this? Because I've been getting questions. Since I no longer work in the DNS industry, I've been getting questions from folks in the financial sector and other industries on this.

JAY DALEY: So we had some in our outputs, but they were done in the fog of – not war, or whatever it was. We have a slide deck that we've just provided to you guys. It could use some work. Like I'm saying, we could use some help from SSAC [inaudible] to figure out, to write something more concise or maybe to point at the other stuff. And then see how we can work to disseminate that. And it may be talking points, it may be presentations, we may get you an interview on CNN. I don't know. Our comms people are available.

RUSS MUNDY: Liman was next.

LARS-JOHAN LIMAN: Thank you. The workshop you mentioned, is that the one tomorrow at 11:00 in [Portopia] coming up with best practices to improve the security in the DNS?

SUZANNE WOOLF: Yeah, it is. I was offering to help. So the way it’s going to run is actually we’re going to talk about first the entire ecosystem of the DNS and what's really basic hygiene. You can take away the word DNS and it’s the same. And as we all know, nobody does anything and hasn’t for 20 years. So I'll be setting the stage for them, Tim and Danny, to talk about as much as they can publicly talk about, given the attacks and really enumerating that the sophistication is because they’ve done their homework, but their techniques are really fundamental.

And then I'm going to close in on talking about specifically credential management, because as SSAC, we specifically did that work on SAC 74, because over and over again, we see breaches where at the heart of it is poor credential management is one important vector. And really, then we’re going to have a discussion. We have at least 20 minutes to have questions and get input from the audience, because I've been doing security for a long time, most of us here have been, and my pet peeve is when people say, “Well, everybody understands best practices,” no they don’t, because there are so many to chose from. So how do we fix that fundamental problem to get people to actually impalement what it is?

And I'll also just point out that there's some really good work that was instigated by ICANN Org to provide a tutorial about credential management. And what's also really nice is they’re looking at community effort for like how-to, how do they do it.

And in Brazil, they did something in 2015 at a registry, and I got permission to actually have ICANN Org put it up on the public site. And it’s how do you implement multi-factor authentication, what are the gotchas, so that other people can learn from their mistakes. So, Tim?

RUSS MUNDY: Yeah, I think Tim was next.

TIM APRIL: Cris reminded me of it as he was talking a minute ago. We had a meeting of a bunch of different trust groups in San Francisco a couple weeks ago, NANOG and [MOG] and all that, where we all started talking about all of this fun. And the consensus in the room at the time was in the certificate system, you have this push-based model with certificate transparency.

There's no equivalent currently in DNS world, where for the longest time, people thought that monitoring their zone was the best thing they could do. It still is the best thing you can do right now, but the only thing you can do where we're starting to come up with ideas and trying to build proof of concepts for what we've been calling DNS transparency. So there's a few of us that have been working on it, we've been talking to some people about how to possibly build this system and what it will look like when we build it. So you're on my list to come talk to you, John, and other people in the room may be interested.

JOHN CRAIN: I love being on your lists, Tim. It's awesome. Come talk to me.

TIM APRIL: There are some of my lists that you don't want to be on, but usually [don't end up there.]

JOHN CRAIN: Okay. Put Danny on this.

JAY DALEY: So, do I have more questions, or can I wrap up?

RUSS MUNDY: Yeah, Rod’s got a question.

JAY DALEY: Okay.

ROD RASMUSSEN: Yeah, so since we’re sitting here with the RSSAC, not just the SSAC in this room, obviously, going after the TLD operators is a really good way. Going after root operators is even better, because there's no parent – I guess they could go after the [dot] so to speak. And I'm sure other folks in the room here have been thinking about this, but what's ICANN, and I guess the RSSAC’s, thoughts on [inaudible]?

JAY DALEY: So we've reached out to RSSAC and asked the question, are there indications? We got back that there are no indications of compromise. It’s interesting communication channels. What we probably need to figure out is, are there other ways? And there are discussions going on with root operators, I believe, as well, [inaudible]. How do we prepare for these things in the future?

And this is nothing on the root ops. We weren’t particularly ready for how this – we've never had to do this before. So one of the things that comes out of this is a whole bunch of lessons learned that we need to do. For example, when communicating with the ccTLDs through their ops list and simple things – and I'm not going to pick on anybody in particular, just the case in particular, if you have a set of contacts that you're expecting to be used for security, maybe you shouldn't use the telephone on your desk in your office that is closed on the weekend.

There will be a lessons learned that a couple of the ccTLD folks are going to write up to pass to that group. But I think in general, what we have there is a really good learning opportunity.

KAVEH RANJBAR: Thank you very much for the update. First of all, I fully understand the need, and I fully support all the education and communication around this to let people know to improve their security. But one part which I have a bit of a hard time with is dealing with this, as you explain, as a crisis from ICANN or communicating it as a crisis from RSSAC, from SSAC or any other organization, because I work for an RIR, and when you were talking about the actions you took, I was thinking, oh, we get so many reports of BGP hijacking, and even if we don't get reports, I have [risks] and I see many of them [throughout the information system,] and I can paint every single one of them as a crisis and say, "Oh, but this happens."

And some of them are governments, armies and things like that. But normally, we tell them, "Hey, this is BGP, this is how it works." There are some security measures, like we have DNSSEC, there we have RPKI and some other that are in different states of maturity. So that's how it works, but yes, that's a distributed system, it has its own issues.

But we definitely don't deal with them as a crisis, although if we want, we can, and that can even extend to ICANN because at the end, RIRs [inaudible]. So I don't see that as a valid path to deal with this, because it's a distributed system, and yes, people will make mistakes no matter what we do.

Communicating, educating, definitely. But calling that a crisis and having emergency actions and things like that, I really don't get how that's justified.

JAY DALEY: So I'm going to respectfully completely disagree with you there, because in this particular case, we are talking about [the attack] being targeted. Target's a funny word because they were really, the tool for the attack were the people that we had the direct contacts with.

I agree if it had been a bunch of companies somewhere that were being manipulated for this, it would have been a different situation. But in this case, it was within the DNS system where we have an SSR remit within our bylaws with the contracted parties, and the noncontracted but where we have a business relationship, like the ccTLDs.

KAVEH RANJBAR: So, same with as an RIR, all of the ASN holders, we have a contract with and we assign the ASN. So in that sense, that's similar.

RUSS MUNDY: Go ahead, David.

DAVID CONRAD: So Kaveh said that the system is distributed. And while it's true that the operation of the DNS is distributed, the DNS itself is hierarchical, and the targets of these attacks were higher up in the tree than they've ever been before, at least to my knowledge. And as a result – no? Okay. I said, "To my knowledge."

So as a result, this seems to be more interesting in terms of response than it would be for an ISP to have their prefix announced because somebody else. I guess your mileage may vary.

RUSS MUNDY: Brad, then Daniel, then Suzanne.

BRAD VERD: Suzanne, you look like maybe you have been waiting longer. Sure. Just really quickly, again, I mentioned – I think I can say this, it's a closed room – the RSOs have agreed to a joint statement that will be published here in hopefully 24 hours stating that there's no evidence of compromise.

Going to your comment, Rod, that the RSOs are the next level up, so maybe we should talk. I think it's an interesting conversation, because the RSOs – and I'm switching hats now, taking off my RSSAC hat, putting on my RSO hat – the RSOs don't – we're not the attack vector here. They serve the root that's provided by IANA, and they have no control or influence on the registry system that is the root.

So it's just something to keep in mind when we think about that.

UNIDENTIFIED MALE: You want to clarify something?

UNIDENTIFIED MALE: [inaudible] the queue.

UNIDENTIFIED MALE: Okay. Daniel.

DANIEL MIGAULT: So, it’s [a little bit unclear] to me which is the target to educate, because in the beginning of the discussion, I thought it was on the [registrar] side, then I think it’s on the zone maintainer, and then BGP, it’s another thing. So what is the target?

RUSS MUNDY: Let’s let John answer that.

DANIEL MIGAULT: The target for education.

JOHN CRAIN: I think that’s something we actually need to discuss, and so I think there are members of our operational community here, obviously some of them are extremely well aware, and others aren't. And there are probably broader communities.

But I don’t think we've answered that question yet. So I think, like I said, there's a lot of lessons learned. This was just the other week, and I think we need to have these discussions. Clearly, there's education needed here, and we need to figure out who the targets are and what the messaging is, and like I said, I would love SSAC's help in that.

RUSS MUNDY: Suzanne?

SUZANNE WOOLF: Sure. Thank you, Russ. I want to go back to the point about communication – and I hate the word "coordination," because there are so many bad things you can do with it, but we'll leave it there for now. But I want to sort of reinforce the point across a couple of angles, and not just with SSAC but RSSAC and all of the players here.

One is that in this particular case, the root servers were not an attack vector, and it would have been nice to be able to say that faster and more effectively just to get higher-quality information out to people about what they should be worried about and what they shouldn't in this case.

The other is that complicated distributed systems are constantly finding new ways to fail, and I think any five of us in this room could come up with 15 bad ideas in five minutes about how the root servers might actually be an attack vector next time, or our infrastructure in other senses might be part of the attack vector next time. And I'm not willing to bet against that.

So we have to be careful how we go about it and managing the relationships and so on, but I think this is a really good example of a reminder that we are, in many senses, all in this together.

LARS-JOHAN LIMAN: I support this. I think the education part is very important. I think it might be a good idea to look at the entire system, but we have to recognize that the attack vectors are probably different at different levels at the tree, and that we have probably different education tasks in front of us aimed at different parties with different content.

JAY DALEY: And there's also the question of who should be doing the educating, right? It's not clear, as the SSR [guy at] ICANN, that we're going to go all the way down the tree. We have our partners in the industry that can help with this.

UNIDENTIFIED MALE: So what's the order? Merike?

AY DALEY: Merike should always go first.

UNIDENTIFIED MALE: Yeah, exactly.

UNIDENTIFIED MALE: So going back to Daniel's question and the follow-ons of educating, for tomorrow – so I'm not saying how you all should do it in the long term, but you did ask about tomorrow. For tomorrow, I'd ask Merike, Tim, and now Danny to focus on things that registries and registrars should be aware of, because that's who we expect to be in the audience, because we're at an ICANN meeting.

Beyond that, that's all fine, but – so if you have thoughts, especially how to do that – because what I'm hoping during that 20-minute question and answer at the end is that we have some registries and registrars stand up and go, "I don't know what's going on here," that would be perfect because that's a good outreach. But for tomorrow, really, what we want is to find registries and registrars who realize that they are offering inadequate ways for the registrants to protect their assets, to go, "Oh, I should be doing better."

So anyways, I just wanted to be clear. That's what I'd ask Merike and Tim to be focusing on, given that that's what our expected audience is for tomorrow. Thanks.

RUSS MUNDY: Okay. Merike and Danny, I think you have the final word on this topic, then we'll close.

MERIKE KAEO: I have a couple of comments on this. One, as John was saying the fundamental attack vectors are not that sophisticated in and of themselves. But what we've seen over the last decade is that anybody creating these attacks are getting much more sophisticated. They are understanding the timings of issues within protocols, they are putting together how routing works and how they can create seemingly correct-looking authoritative servers that have the right IP address, just doing route hijacks.

So with all of the breaches that have been going on for the last decade with all of the credentials, my worry is that the entire Internet ecosystem doesn't have safe credentials. So with multi-factor authentication, I'm not that worried because I know that they don't have the second piece that they might need.

And people are kind of saying, "Oh, don't panic. Oh, there's no crisis." But we see the sophistication and the impact keep increasing. So, are we ready? And I come from a small country, Estonia, that had a very significant attack in 2007. If they had not been lucky enough to have at the last minute almost created a trust relationship with the global security operators, that country would absolutely 100% have been down. And it was purely serendipity. And I speak as somebody that's very aware of this.

So I'm concerned with the lack of, in some way, urgency. And I can tell you that now as a member of the board, this has been discussed, and really, we're trying to figure out what is the role of ICANN in an ecosystem – because we're not alone, just as Suzanne was saying. We need to figure out how does ICANN play a role in this. It has a very significant role when you look at the DNS ecosystem.

And my worry is, globally, that people are always punting on security. "It's not so bad, not my problem." And I think the time has come that we really need to take a close eye on, well, if I'm running a server, I don't care what you're operating, are you doing the best hygiene on your servers?

And I can tell you a lot of people aren't. They should know better, and they're like, "Oh, yeah, I didn't do that. I should." So look to yourselves and see how you're operating your infrastructures. Maybe you are perfect. Maybe you've got everything in place. I kind of doubt it.

So I really would ask all of you, let's look at what is our role in this, and figure out how we can each help the entire ecosystem.

RUSS MUNDY: Danny?

DANNY MCPHERSON. I saw the communications that went to one of the ccTLDs that was impacted by a compromise of one of their authoritative servers, and there's a lot of misinformation in that. And most of that misinformation was aimed at deflecting responsibility from the person that operated that infrastructure and suggesting that the entire DNS was unstable and insecure.

So for that reason, I think that the outreach that ICANN did and the recommendations that they made were really important, because I know that [went to] a lot of others.

I think that that same entity did a lot of things publicly and made these things sound really sophisticated when a lot of basic hygiene, blocking and tackling on their behalf would have probably mitigated most of this attacks surface anyway. Not to say that there weren't other issues and things that should be done.

So I think for that reason that it was really important that ICANN say something in that respect. We saw emergency root zone changes come in and changing root zone infrastructure for a country, and it was based in part on false information that was later, in part, cleared up.

So I think for that reason alone, it was really important that ICANN did what they did. I think the timeliness of a statement, at least from root ops if not from other impacted parties, would have been really helpful for ICANN, and some maybe better coordination between staff and the operation side, at least at the root zone level to make sure that those were coordinated would be really helpful for everyone. And I know that Dave and some of the other folks are talking about how you improve that.

And then to Merike's point, I think that some of the entities – not all the entities, but some of the entities – involved with this – I don't know if you've heard, but someone asked at one point what's an APT, an advanced persistent threat, and someone replied that, "It happened to me."

So I think that some people were making these sound much more sophisticated and deflecting to other parts of the ecosystem rather than owning the changes and the things they should have implemented themselves. So for that reason, I think what ICANN did was valuable.

KAVEH RANJBAR: Thank you, Danny. That resolves my concern.

RUSS MUNDY: Okay. Thank you, everybody. This has been a very invigorating session. I hope everyone has found it worthwhile. I usually ask for a little feedback at the end, but we're already four minutes over, so I won't, but I will ask if anybody has feedback, send it to me or send it to the full list of whichever one.

One quick question, does everyone think we want to have another similar session in Marrakech? Yes or no. Yes. Okay, we'll take that guidance. Thanks, everybody. Enjoy lunch.

**[END OF TRANSCRIPTION]**