Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
26 January 2012 at 14:00 UTC

Note: The following is the output of transcribing from an audio recording of the DNS Security and Stability Analysis Working Group (DSSA WG) teleconference on 26 January 2012 at 14:00 UTC. . Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at:
http://audio.icann.org/gnso/gnso-dssa-20120126-en.mp3
Presentation will be posted shortly on:
http://gnso.icann.org/calendar/#jan

Attendees on the call:

At Large Members
. Cheryl Langdon-Orr (ALAC)
. Olivier Crépin-Leblond (ALAC) (co-chair)

ccNSO Members
. Takayasu Matsuura, .jp
. Katrina Sataki, .lv
. Jörg Schweiger, .de (co-chair)
. Jacques Latour, .ca
. Wim Degezelle, CENTR

NRO Members

GNSO Members
. Mikey O'Connor - (CBUC) (co-chair)
. Rossella Mattioli - (NCSG)
. Rafik Dammak, GNSO
. Scott McCormick (IPC)

SSAC Members

ICANN Staff:
Glen de St Gery
Julie Hedlund
Bart Boswinkel
Patrick Jones
Nathalie Peregrine

Apologies:
Rick Wilhelm, Network Solutions
Don Blumenthal - (RySG)
Mark Kosters (ARIN); (co-chair)
Edmon Chung - (ALAC)

Nathalie Peregrine: Thank you Tim. Good morning, good afternoon, good evening. This is the DSSA call on the 26th of January, 2012. On the call today we have Mikey O'Connor, Cheryl-Langdon-Orr, Rosella Mattioli, Joerg Schweiger, Rafik Dammak, Takayasu Matsuura, Olivier Crepin-LeBlond, (Kurt McCormick), Jacques Latour, Katrina Sataki and Wim Degezelle.

From Staff we have Glen de Saint Gery, Julie Hedlund, Patrick Jones, Bart Boswinkel, and myself, Nathalie Peregrine. We have apologies form Mark Kosters, (Vic Wilham) and Edmon Chung.

A note from Don Blumenthal who might be arriving late. I would like to remind you all to please all state your names before speaking for transcription purposes. Thank you very much.

Mikey O'Connor: Thanks Nathalie and welcome everybody. We've got sort of an interesting agenda today, partly because I've sort of tripped over the fact that it may just be that the way we're tackling this doesn't scale, and so I want to try some ideas out on you all.

So for those of you who are waiting in breathless anticipation to vote, rest assured that we will be doing that. But before we do that I just want to take a small detour to touch bases on a couple of things.

What you see on the screen right now is that little architecture diagram that I sent out to the list earlier this week. And the reason I want to very quickly go through this is because - well because of this.

Let me show you the other thing that I'm working on, and that may be a little too small. Let me - I'm going to make it bigger in a sort of - what's happening I think is that we've - well I can't do that.

Sorry. We've got a permutations and combinations problem where we've got a series of four layers that if we evaluate all permutations of all layers, we're going to wind up having thousands perhaps of threat event/threat source vulnerability and then it goes on.

I just stopped drawing the drawing at that point, combinations and permutations. And so I think that what we need to do is step back and say, "All right, at each stage of the game what we're really about is sort of pruning off branches on this tree."

And it's not that we'll ignore them. I think what we need to do is document them, but I don't think we can evaluate them all. I think we have to basically create the tree and then say at each stage of the game, "These are the ones that appear to be the most important to us right now."

And so those are the ones that we're going to go into a detailed analysis of, and we'll leave the rest of the tree for another day. And it could be a subsequent group or it could be a change in circumstance that says, "Well this threat source that we didn't think was a very big deal has suddenly turned into a very big deal, and so we need to come back and do the full analysis on it even though the folks back in the original DSSA did not.

Now it's important and we need to do the detailed work." I think what we do is we leave behind the framework that makes it easier to do that, but I just don't think we can evaluate them all.

And so I just want to take a moment to go to the beginning of that tree, which is really the architecture, the big pieces of the DNS, and first make sure that

we've got them all because it's from these things that the threat events come from.

So for example just sticking with our Major TLD Zone and the zone file of that zone, then from there comes the threat event, that zone file gets disrupted somehow by a threat source whether it's malicious or not.

The ones that are in green are the ones that we've already put into our list of threat events. Let's see if I can get to the table real quick. I'll make this a little bit bigger so that you can see it.

But here are the threat events that we've already evaluated, and you can see that there's basically a one to one mapping between that list and the green stuff that's on this page.

So for example support files we just evaluated at its - at this level. We didn't go all the way down to the kind of support file. We left those as a blob underneath it, whereas with the zone files of the TLDs we went one layer down.

We did the zone file, the DNSSEC and the Registrar/Registrant provisioning and we did that last one primarily to annoy Joerg and get his blood pressure as high as possible, which I think is a very important piece of our work is to keep Joerg's blood pressure pretty high.

But the rest of them at one point or another we thought were pretty important. When I went back and said, "Well what about the Root Zone? Are there - is there a parallel set of things for the Root Zone?"

I just didn't know the answers to those so there are question marks besides these over here, because I am not that familiar with those kinds of parts of the DNS.

And I just wanted to very quickly see if we needed to add an analysis of say the DNSSEC for the Root Zone. I'm pretty sure that the Root Zone is signed but I wasn't sure enough to take my question mark away.

So I just want to pause at this point before we dive into this and see if people are following what I'm saying, if you have questions about what I've said so far.

Not seeing anybody's hand go up so I'm presuming I'm okay. What I'd like to do is just very quickly see if we need to put out threat events for the DNSSEC.

I'm just going to do these one by one, and I think what we'll do is we'll just use your checkmark agree signal if you think we should take a look at the threat event that says the DNSSEC for the Root Zone gets disrupted.

And if it is then we'll stick it into our list, so with that how about it? DNSSEC on the Root Zone - A, does it exist; and B, should we evaluate the, you know, the - essentially the impact of it? Patrick, go ahead.

Patrick Jones: Thanks Mikey. Patrick Jones for the record. Well the root was signed in June and July of 2010 so it's there. I mean, I think we need to consider it. I sent to the ops list yesterday, and I probably should've just sent it on to the whole DSSA, the example from NASA.gov having a key issue.

And Comcast has, you know, done a nice write-up on what happened, and I believe it's public. So, you know, this is an example of the, you know, risks of and the brittleness that may be introduced as more and more zones start using DNSSEC and more second-level use becomes used to it.

So it looks like yes, Roselle has posted the link to it so that's very helpful. So this is the type of thing that the group should talk about.

Mikey O'Connor: All right, well we'll put it in the pile. I can't quite remember how I - do a short pause while Mikey learns his tools. Can't remember how I formatted this thing.

I will just use checkmarks for now. I'll go back and fix that later. So this one gets in. How about the provisioning of the Root Zone? That - this is the parallel to the Registrar/Registrant provisioning.

Are there provisioning systems and if they were disrupted that's something that we should - well let's just stop with the - are there provisioning systems?

I didn't know. I didn't know if that was a manual process or a highly automated process. Anybody who's familiar with the Root Zone want to weigh in on that?

Patrick, are you close enough to the Root Zone to know how it's provisioned?

Patrick Jones: Well I think someone from one of the root operators should speak to this, so while ICANN does operate L-Root I'm not on the L-Root DNS ops team. So I'd rather have someone that is part of one of the root operators talk specifically about this.

Mikey O'Connor: I don't know if we've got any of those folks on the call. May - we may want to leave this one for - well Patrick, I'm going to pin you to the table like a butterfly because we don't have anybody else from the root operator on the call. What does L-Root do? Does that have automated provisioning?

Patrick Jones: Before I answer that I want to defer that to the DNS ops team, so I can either check to invite, you know, Joe Abley or someone from his group to be on next week or we could see if there's someone else from one of the other root ops that appears on the call. Too bad Bill's not on the call today because this is right up his alley.

Mikey O'Connor: Yes. I think I'll put that on the - let's check back later. And, you know, the question - it's really a two part question. One part of the question is, is there automated provisioning?

It sounds like it's different for each root so it would also be interesting to know whether it's the same system or not.

Patrick Jones: Yes, my expectation is that it will be different for each operator and not all of them use the same software and steps, and that's partly what makes the root operators resilient and that they do have some uniqueness.

Mikey O'Connor: Right. Yes, heterogeneous systems. Okay. We'll leave that one for now. So then the next four are the WHOIS zone file access data escrow and bulk data access.

It seems like WHOIS doesn't exist at the root but I didn't know, so I thought I would ask. Anybody want to educate me on that one?

Patrick Jones: Mikey it's Patrick again.

Mikey O'Connor: Way to go Patrick.

Patrick Jones: Yes. So there is a, you know, IANA does have a WHOIS database but - and it's too bad that Mark - not what Aaron does with their, I mean, I'd say unless there's someone else on the call that wants to talk about this, you know, defer it to next week as well.

Mikey O'Connor: Okay. That may be what we should do. I tell you, I'm thinking we're going to have this same conversation all the way through this list, so rather than drag us bumping and screaming across all that pain, I think what I'll do is I'll just punt this back out to the list with some more specific questions so that smart people can just answer them on the list.

Okay so let's then go to the next change that I want to propose, which is that I'm - no actually it may be easier to see here. I'm thinking that if you look on this line map these are the threat events that we've evaluated so far against the threat source configuration users by privileged users.

And as I went through that architecture thing I decided it might be useful to make those more generic so that they could apply to different sources of threats, because these don't really make sense when you make the sentence, a business failure of a key provider and, you know, if I put that part of the sentence together with this description it doesn't make sense, because this sentence includes the configuration error.

And so what I did is I made more generic versions of all these so that then when we go through all these other threat sources, we get sentences that make sense.

And so a business provider fails which disrupts a Major Zone file. A business provider fails and the Root Zone is not published. A lot of these, you know, still work as sentences but I think we can pretty quickly eliminate a fair number of them.

But before we went through and did all the voting I wanted to make sure that this generic version of these conversations that we've already had make sense.

They make sense to me but I didn't want to just spring this on you without giving you a bit of a heads up that that's what we're doing. So again here I'm just sort of looking for cries of anguish that this is a bad idea.

And if it's okay then we'll just keep going. Any thoughts on this one? The generic word overhaul - yes, you know, this is part of that process that we went through last time where we ultimately said in our update to the community we didn't have time to make it simple.

I think as we make these more simple they become more powerful. So okay, so I'm going to take that as a tentative okay. I'll highlight that we did this to people who aren't on the call on the list, and allow cries of anguish on the list as well.

But for now this is the way we're going to do it. Now I want to just go through one more piece of checking with you before we carry on. Essentially what we've done in this table is we've made the permutations mistake, because instead of evaluating just the list of threat events - let me go back to the line map here for just a minute.

What the methodology says we ought to do is we ought to just take a look at the threat sources, and we ought to evaluate the range of their effects. So you can see down in the little pod that I'll just move around so that you can see this pod.

That's the pod that's range of effects and that's what we're supposed to evaluate the threat sources against. And the methodology doesn't have us doing the permutation business that we invented.

And the reason we invented it is because we said, "Well look, configuration errors by privileged users - the range of effects varies depending on which threat event happens."

So - and that's where we went off into the permutations thing. That's the good news. We get much more granular data and we get much better evaluations.

The bad news is that we run into this scaling problem if we're not careful. And so what I'm thinking we might want to do is go through maybe one or two more of these really detailed ones, and then step back and see whether we can revert to just evaluating the threat sources with their range of effects.

We may not be able to do this but if we can't we're going to take a really long time to get through this work, and so I just want you all to be aware of the kind of balancing act that I'm working on right now.

And so if some of you are feeling sort of dragged through this too quickly, the reason is because I'm trying to scale back the amount of work that we do to a point where we can get it done in a reasonable amount of time.

And this is something that sort of came out when I was starting to prepare the slides for the updates in Costa Rica, and so my co-chairs haven't even seen this.

And if you're all sitting there going, "Where in the heck did this come from?" it's because it showed up between Monday and Thursday. So with that off we go.

We're going to start voting again and I think that I'm going to just do it on the table, because the table is now starting to be a better way of displaying what we already know.

You know, if we do the comparison between these two is it safe to say that - and the reason that I think that we might be able to chop this back is that once we've done a couple of these we may be able to say, "Okay, the threat event where a Major Zone file gets disrupted has a pretty high relevance," which is what we're supposed to be evaluating these on.

So we'll just see how this goes and if it doesn't go well we'll fix it again, but that's what I'm trying to fix. So Nathalie now we are going to zoom off and start doing the voting.

The first sentence that we're going to vote on is this one, and I hope that you all can read that on your screen. It's a little bit smaller so if it's too small let, you know, just give a shout.

But if it's okay I think it's useful to do it this way. Rosella is saying too small. Okay so let me go up a notch and see. I've got a tradeoff here of what to show.

And I can't show what I want to show which is I want to be able - to show is the comparison between - oh no, I guess it's on there. All right, so we'll do - this is the one we're doing but I've got the Row 6 one up there so that you can see how we voted on its last incarnation.

So the first question is what's the range of effect if there's a business failure of a key provider, which in turn disrupts a Major Zone file? So this is the pod on the left, the range of effects.

So 10 is a sweeping all the way down to 1 which is minimal. So now it's time to use your little scales and start voting. Don't all vote at once. The lack of voting meaning that I've totally confused you?

If so I could try it again. There we go. People are starting to vote now and remember this is a Major Zone file goes away because of a business failure of a key provider.

And I guess the question that comes to my mind is why is it then when a Major Zone file goes away because of a configuration error, why is that different than when a zone file provider goes away? The zone file's still gone. Go ahead Patrick.

Patrick Jones: Yes, so maybe I'll jump into this one. If it's a business failure of a large zone operator the zone's probably not going to go away. They'll be either the operator will have made arrangements to transition that, or it's at least preserved the TLD in the zone until it - a new operator can be found or something will happen so that the names will still resolve and business can

still be conducted even though there may be a business failure. You know, I might be wrong. So it looks like Olivier wants to talk as well.

Mikey O'Connor: Yes, go ahead Olivier.

Olivier Crepin-LeBlond: Thanks very much Mikey. It's Olivier here for the transcript. I'm working from memory here but wasn't there an arrangement for escrow to be used in case a business failure happens a zone can be immediately transferred elsewhere, or am I just having some wishful thinking at the moment?

Mikey O'Connor: Yes I think that's at the Registrar level for sure. That's the Registry - Registrar fly or Registry fly.

Patrick Jones: Yes, so this is Patrick again. You know, at least in the generic space all the Registries do escrow their data and if there's a serious enough failure where we needed to go back to the escrow data to recreate a TLD zone it can be done.

We've tested it with certain operators and it can be done. That's pretty extreme though. I think in most case where there's a business failure there'll be a transition.

The, you know, one thing to keep in mind is that we really haven't experienced this with a key provider. There have been smaller operators that have been transitioned from one operator to another, or there have been many examples of TLDs that have been acquired and changed hands and there's been no notice at all by the community.

So a couple of examples come to mind. Dot name was acquired by VeriSign. VeriSign ran the back end. They transitioned the operations of the business. Nobody noticed.

You know, org was transitioned from the, you know, original operator which was VeriSign as well to PIR and it's too bad Jim's not on the phone to talk about that.

But Don's on and, you know, there is no loss of service for dot org users when that TLD was transitioned from one operator to another. So - and that wasn't a business failure but it's just an example of transitions of zones. And I see Joerg wants to talk as well.

Joerg Schweiger: Yes, it's Joerg.

Mikey O'Connor: Go ahead Joerg.

Joerg Schweiger: It's Joerg for the transcript. As far as I know escrow will definitely be mandatory for the new gTLDs. As far as ccTLDs are concerned I think we are not obliged to escrow our data and for example dot e is not doing so.

So we could not assume that escrow will be available for each and every Registry. Nevertheless I think Patrick was absolutely right referring to the fact that even if there would be a Registry failure then the zone file would probably still be available, or it might be available in part of an older version.

So it wouldn't be so effective all at once and due to that fact I think we could explain why the voting is probably a little bit lower than we saw with the zone file directly. Thanks.

Mikey O'Connor: Yes, and see this is where the problem comes in with what we're doing, and that is that what we're really doing is we're saying - we're talking about what we think the likelihood's going to be.

And what we're saying is we think the likelihood of the zone file going away is very low. And the question that's really being asked is not the likelihood question.

That's going to come later in the analysis. The real question is what's the range of effect if it goes away? And it seem to me that the range of effect is the same, which is if it went away it would be exactly the same effect as if it went away from any other cause.

And so while I will dutifully record this, this is the puzzler that I'm trying to work my way through is how we avoid conflating the analysis that's to come, which is the likelihood one with this early one, which is just trying to understand the range of impact if it happened.

And I'm a little concerned that what we've just said that if its own file goes away under one circumstance and has a big impact but if it goes away under another circumstance that has a small impact because in both cases it's gone away.

So that's the puzzler that I'm sort of chewing on in my mind. But I will record it and not get us any more stuck on this because it's important to keep going.

All right. So right now we have - where am I here on my little chart. I'm going to switch over to recording here and seven votes for that. Okay. So the next thing to vote on...

Olivier Crepin-LeBlond: Mikey, it's Olivier.

Mikey O'Connor: Go ahead.

Olivier Crepin-LeBlond: Thanks, Mikey. It's Olivier for the transcript. I'm a little confused. Now you said a small impact but we voted five which is wide-ranging involving a significant portion of this cyber resources of the DNS. That doesn't look too small to me.

Mikey O'Connor: No, but it's smaller than what we voted up here...

Olivier Crepin-LeBlond: And we're on the eight...

Mikey O'Connor: We're on the higher side. We were on the sort of eight to ten-ish. Mostly eight range and that's what's puzzling me about this is that it would seem to me that the range of effect of the loss of a zone file is the same no matter what the cause of that is.

Olivier Crepin-LeBlond: Maybe we're just psychologically getting used to threats.

Mikey O'Connor: That's right. We're getting immune. And so I think we have to puzzle about this. Maybe the (code shares) can (unintelligible) up at this.

Cheryl Langdon-Orr: Actually...

Mikey O'Connor: Cheryl, go ahead.

Cheryl Langdon-Orr: Cheryl here. Actually what Oliver said although in jest is probably quite accurate. When you're looking at files that are actually as close as that, extensive and wide-ranging, our (patch ill) design turns in some of our minds compared to others.

When you hear something that is not quantitative metric but rather a qualitative terminology, you will get drift between one set of input through (unintelligible) characters between sessions. That's what statistical variation is all about. You have to do a non-parametric analysis to avoid that or use only quantitative terms, not qualitative.

Mikey O'Connor: Yeah. Yeah. Well, it's just a puzzler. We'll keep going this way but I have a little scratch on my head both on the scaling problem and on the drift problem. I think we may have made a pretty fundamental error in combining these two into one table. But there you go.

Okay. So now we're onto the relevance vote which, again, is the confirmed all the way down to possible scale. And so this is one of those questions. Have we seen a major zone file go away and maybe this is the place that I would be more comfortable with a pretty low vote.

So then what we can have is the range of impact would be the same but, you know, perhaps this sort of predicted versus confirmed thing is where we embed the conversation about, you know, the - well, really the whole conversation about the safeguards that have been put in place.

And almost what I'd like to see us do is not vote on the range of impacts with each one but just vote on the relevance which is the scale for the thread events that we're working on.

So, anyway, people are voting, that's great. I'm sort of being like a radio announcer and providing filler commentary. And meanwhile I want to get into the chat.

And Jacques is saying I think the context for this is a threat for a large deal to go out of business unexpected. Supposed to a malicious and natural disaster recoverability of its own. Jacques, are you able to jump on the bridge and unpack that one for me a little bit? I couldn't quite get what you were getting on that.

Oh, no talk. All right. Well, we'll give you a little time to type more slowly and maybe you can just stick a few more words into that. I get the no talk problem.

Meanwhile, we do seemed to have put this at a pretty low-end of our relevance scale which makes me quite a bit more comfortable because what this would do is it would knock this pair out of our subsequent analysis. Basically, this is the pruning that I'm hoping to see so that we can wind up with not quite so many branches of our tree to analyze later on.

And so I'll record that and we'll move onto the next one which is the disruption of a lesser zone file by business failure of - in its parallel one up on line seven we said that the range of effects of this would be pretty low. We tended to cluster around the three.

Let me clear the voting so that we can start voting on that. So this is the disruption of a lesser zone file due to the business failure of a key provider. And, again, my tendency if I was to do this - I'm not voting as you may notice - but my tendency would be to go up and look at the vote that I did before and echo that because the range of effect of a lesser zone file going away would seem to me to be the same.

And then the relevance which is the one that's really tied to the business failure version of this, is where I would swing my vote. So with that people are voting. Let's see. Patrick's talking about the KPN Quest bankruptcy. Yeah, and there was...

Patrick Jones: Mikey O'Connor, Patrick Jones again. So I have - I have to dig up the write-up on this failure but there was a pretty major bankruptcy for KPN Quest right around the dot com boom and it did have some impacts.

I'm not going to describe it in the proper context so what I want to do is go back in file and pull out something I can then send to the list that provides more detail.

If there's anyone else on the call remember this example and can talk to it and provide more detail please do, otherwise, I'll just go back and pull up the record. From what I recall this did have some impacts that were not expected. So let me send that to the list.

Mikey O'Connor: Thanks, Patrick. Meanwhile, folks continue to vote away. We've got three of our seven voters in there right now. Going once, going twice. And recorded

as six votes for three. Okay. We'll call it six for three. Whoa, it's red. I don't know why it's red. Artifact, something. All right.

So then the question is where Patrick's comment I think comes in which is the relevance. Have we seen it? And what Patrick has just said is yeah we have seen that.

So we still probably wind up with this not floating to the very top of the hit parade because it doesn't' have a huge impact but it's quite relevant because we've actually seen it before even - either ICANN has seen it or our peers and partners have.

So the votes are coming in at around eight to ten and then Bart's got a comment. KPN Quest is an interesting example of what happens. The first thing that happened was that the caretakers came in and what happens next will depend very much on national law provisions. Oh, that's a good one. I'll just steal that one for my little - keep voting I steal this. Staple it in for our (unintelligible).

Okay. So we're up to five votes. Getting ready to record this one as four votes for ten. I don't know why these are coming up red. I'll have to go figure out what I did. Sort of (fell) artifact. Okay.

The next one is when a business failure of a key provider causes the root zone to be published incorrectly. This one I've sort of combined two of these and said that are sort of simpler more generic version of this is that the root zone is published incorrectly.

And then the next one is it's not published at all. So with that carry on with the voting. First is the range of impact one. And we'll evaluate the impact range of effect of the root zone being published incorrectly. Go ahead and vote.

Oh, I like the animation. That was neat. Okay. We're up to six. I'll call it done at six. We started having seven votes but we're pretty consistently down to six more recently. So we have one, two at ten, three at eight and one at five. Okay.

And then the other question which is the relevance. So this is confirmed, it's actually been seen all the way down to possible described by a somewhat credible source. That would be me. I'm thinking of Mikey as a somewhat credible source.

So, what do we think the relevance is. Go ahead and vote. Now remember this is the root zone being published incorrectly because of a business failure of a key provider. So that would have to be a provider of the root zone. One of the however many it is. Okay, we seemed to have honed in on three for that one. Going once, going twice, getting ready to record it. It's up to six.

All right. The next one is the same question, same pair of questions except the root zone is not pushed at all due to the failure of a key provider. So this would have to be some sort of ripple effect between the providers so as one of them failed they took down the root zone for the rest and the range of impact would be pretty dramatic, at least the early voting has it that way.

And that's our six so I'm going to record it. And then the relevance one - no we have seven. We're back to seven. Sorry. I missed that last vote coming in. Okay. Clear these.

Now the relevance which is the confirmed all the way down to possible Go ahead and vote on the...How often we've seen that ripple effect actually happen. Wow, that was quick. Okay, now we're rolling. So we have seven for the one. Next one. Same sort of thing except now we're talking about the IANA zone file.

Olivier Crepin-LeBlond: Mikey...

Mikey O'Connor: Go ahead.

Olivier Crepin-LeBlond: It's Olivier for the transcript. I noticed that in earlier instances we actually noted zero as well but now in these threat events relevance we don't have zero so I wonder - I was rather tempted to vote zero on this one.

Mikey O'Connor: That's interesting. It might be tricky with the PODS. Oh, shoot. Have I done that major confusion thing? Hang on just a minute.

Cheryl Langdon-Orr: Cheryl here for the transcript record. I think we did discuss this and if they have been adrift away from the zero and I thought the reasoning was once we cleared up what we meant by relevance and the range of effect and that's where we had those (unintelligible) earlier on. In under relevance it would to (be) zero, it would have to be an impossibility and the impossibility of a threat - I wouldn't think there'd be many (unintelligible) votes that it would be impossible.

Mikey O'Connor: You know, I just can't remember.

Olivier Crepin-LeBlond: Olivier here, I've got a zero earlier at the root zone misconfigure the IANA zone file.

Mikey O'Connor: Yeah. And I don't want to - I think the zero goes with the range of effects. I think it goes over here but I can't remember.

Cheryl Langdon-Orr: It could go with the range of effects but it's recorded in the relevance and I think that's an artifact of us having the (muddy) waters early on. Sorry, that was Cheryl for the transcript.

Mikey O'Connor: I'm going to type it in and I will check after the call to make sure and we'll record the zero. I can't remember. I can't remember. Sorry. That was a goof. My fault. Okay. So now we're on to the IANA zone. We might be able to get

through this whole chunk today if we chug right along. Olivier, is that an old hand or a new one?

Olivier Crepin-LeBlond: That's a new one, Mikey O'Connor. I'm sorry. You've added a zero there but you didn't take - you now have right votes on this and in fact my vote was originally a one. That (would be) to two zeros so back to six.

Mikey O'Connor: Good god, my computer's going crazy. There we go. All's square. Okay. On to the IANA zone where again we're going the range of effects. If the IANA zone goes away and in this case - Patrick, is there only one provider as IANA handed off across multiple providers too? This is another one of those architecture questions for you. Is ICANN the only publisher of the IANA zone?

Patrick Jones: I believe that's correct.

Mikey O'Connor: Okay. So this would be...

Patrick Jones: So this one is a business failure of ICANN.

Mikey O'Connor: Yeah, that's what I was trying to get at.

Patrick Jones: Until or unless there is a change of provider of the IANA functions in the future.

Mikey O'Connor: Yeah, right. The range of impact if the IANA went away is what we're working on right now. And then in a minute we'll take a look at the relevance but let's do the range of impact first.

We've got a couple of votes that are pretty high if it went away. Finish that out. It's climbing slowly, there we go, up to five, six. Going once at six. Call it six. Poor Jacques. Too bad that you're not able to talk, Jacques. I see him typing in the chat.

Okay. So ignore the red and let's go on to the other half of this puzzler which is - what's the relevance. So this is the scale on the right side confirmed down to not applicable. And pretty solidly at one. Going once at five votes for one. Anybody want to drop a couple more on the thing before I record it. There we go, seven.

Okay. Next one is the DNS sect is disrupted from a major provider. And first is range of effects and this is where that NASA story is pretty interesting. Just to recap it a little bit NASA misconfigured their DNS sect and Comcast dropped their - in that case I think it was the second level NASA.gov domain out of their DNS and stopped delivering traffic to that which made it appear that Comcast was blocking it when in fact what was going on was the DNS sect had been misconfigured.

So that's one layer lower than what we're looking at. It certainly had a profound impact on NASA. So that's the description of the event. And the question would be what would the impact - the range of effects be if that happened to a major provider.

You know, a major provider had a business failure and this would probably be DNS sect for the dot com zone for example or the dot DE zone if it was signed. Joerg, I don't even know if dot DE is signed.

And it would seem to me that if the thing that happened with Comcast was true then what would happen is that that zone would go away for a lot of people because the DNS would interpret that as, you know, an invalid zone. I mean, that's the whole point of DNS sect is to authenticate and verify the veracity of a given domain.

So my thought would be is if it was a major zone it would be a big impact. It would be pretty much on the same level as losing the zone for anything else. So there's my color commentary while you all are voting.

We have four votes so far. We have actually our first fairly wide spread difference of opinion. Whoever voted one do you want to chime in and try and lobby the rest of this as to why you think it's not a big deal?

Oh, Jacques. Oh, well. We'll save that one for another day when you can talk on the phone. I'll just record it for now because it's really hard to carry on that kind of conversation with...

Yeah, but the trouble is that it's deployed on major zones and so as it gets deployed at the other end, at the ISP level - I mean, the thing that's interesting is the role of ISP is in this.

And as they get more and more savvy to the DNS sect on their end it seems to me the impact goes up but that's a darn good point. I will add that to our notes while you're voting. Not that way. This way. Okay. I'm going to go back and record this one with...Bless you. Jacques, did you take your vote down or do you want to...

Cheryl Langdon-Orr: Mikey, stop trying to manip...

Mikey O'Connor: I didn't do it. I just wanted to make sure I recorded it right. Okay. All right. So the next one is the relevance one. We've seen it all the way down to - described by somewhat credible source and I think the answer is we've certainly seen it at the second level because that's Patrick's example.

Whether we've seen it at a major provider - and again, this is due to business failure. Not all cases but this is - if there's a business failure and Patrick's example is it wasn't a business failure, it was a configuration error. It was more the one we were working on the last time. This would have to be a bankruptcy that takes down the DNS sect for a given major zone rather than a - well, I seem to be confusing the issue.

We've not got a pretty wide - let's see if we can have a bit of a conversation on the call about why we are so spread on this one. We aren't honing in, we're actually spreading apart. Anyone want to chime in as to why you voted the way you did?

I don't think that we've seen this before where a business failure has caused this. So I'm curious about the voted who voted...

Cheryl Langdon-Orr: You're losing people left, right and center.

Mikey O'Connor: Oh, god, it's 9:00. Sorry. Okay. We'll just stop right here. I'll record it and we'll pick up the conversation at this point. Thanks, Cheryl, for the heads up. See you all next week. We're chugging along.

Cheryl Langdon-Orr: Thank, Mikey.

Mikey O'Connor: That's it for me.

Cheryl Langdon-Orr: (Unintelligible).

Mikey O'Connor: Okay. We can stop the recording.

Woman: We're turning off the recording.

END