Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
19 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 19 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-20120119-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)
• Andre Thompson (At-Large)

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

NRO Members
• Mark Kosters (ARIN); (co-chair)

GNSO Members
• Mikey O'Connor – (CBUC) (co-chair)
• Rossella Mattioli – (NCSG)
• Don Blumenthal – (RySG)
• Rafik Dammak, GNSO
• Greg Aaron – (RySG)

SSAC Members

• Jim Galvin (SSAC)

ICANN Staff:
Bart Boswinkel
Patrick Jones
Nathalie Peregrine

Apologies:
Julie Hedlund

Coordinator: We're now recording.

Nathalie Peregrine: Thank you (Ricardo). Good morning, good afternoon, good evening. This is the DSSA call on the 19th of January 2012. On the call today we have Mikey O'Connor, Cheryl Langdon-Orr, Andre Thompson, Rafik Dammak, Olivier Crepin-LeBlond, Rosella Mattioli, Takayasu Matsuura, Wim Degezelle, Katrina Sataki, Jim Galvin, Roy Arends, Joerg Schweiger, Jacques Latour, Don Blumenthal and Greg Aaron.

From Staff we have Bart Boswinkel, Patrick Jones and myself, Nathalie Peregrine. And we have an apology from Julie Hedlund. I would like to remind you all to please state your names before speaking for transcription purposes. Thank you and over to you Mikey.

Mikey O'Connor: Thank you Nathalie. Capital letters, gad what a jerk. Thanks all for joining. Just a quick operational note before we get underway. You will notice that the format of the mind map on the screen is a little bit different today, and that's because I am switching over to FreeMind, which is the open source version of the tool that I was using before.

And so I apologize in advance if I spazz out really badly. I'm sort of four days into learning this tool, but the advantage of using this tool over the one I was using is that it's available at no charge and so we aren't quite so constrained as to who can read and operate the maps.

So if you would like to join the FreeMind conspiracy, I've put the latest versions of all of our mind maps or at least most of our mind maps up on the Wiki in both the old format and the new.

And there's a link on every page to the FreeMind site, so you can go off and download a copy for yourself, open these things, play with them, et cetera. And so that's just a quick operational transition.

A quick note of thanks to Olivier for running the call last week. I actually thought the call went spectacularly better with the two of us doing it, and I think that Olivier is going to run the call next week so we can kind of compare.

But we're back to all Mikey all the time this week, and just to replay the bidding I went ahead and changed our table to summarize the results from the last call.

And just for those of you who missed it, we had a pretty long discussion about my mistake in which I had us evaluating likelihood, when in fact we are evaluating relevance.

And I won't replay all that bidding but if you're confused by that and you want to visit a little bit after the call, I think it'll make sense to you as we go through the rest of this.

But feel free to hang on the call a little bit and I'll replay the conversation we had about that. But we are evaluating this a little bit differently so if it feels odd to you, you're not crazy and hang in there for a minute and I think it'll be okay.

Where we left off is - just to put this in context I want to show you sort of where we're at in the whole process. Right now we're working on non-

adversarial threat sources and we have about, I don't know, eight or ten of them.

You can see them there. And the one that we've been working on is configuration errors by privileged users. In there we have about five or six that we've evaluated, so we've got a ways to go even on non-adversarial threat sources.

And then we get to the adversarial ones, which are the ones that are sort of flashier and so I just wanted to sort of remind us of the context of this conversation.

Where we're at right now is in - oops, that wasn't what I intended to do. In configuration errors by privileged users we've got these - highlighting things is going to be tricky.

Let me try - there we go. We've got these that we've finished and they're mostly - well they're all about Root Zone file. Where we got - where we stopped is basically the question that's been going on on the list, and this is part of my secret conspiracy to answer this question, which is what other kinds of files - we started with DNSSEC files, but what other pieces of the DNS should we include in this list?

And that's why I launched that conversation about the definitive list of stuff that's in the core registry services. So for a minute what I'd like to do is just see if there are any more chunks of the infrastructure that we should include, or whether we should just stop at the Root Zone file.

And I think I'd like to refer you mentally back to that conversation we had on the list where we were talking about, "Well, is EPP included? Is WHOIS included? What's in and what's out?"

And I'm kind of looking to folks like Greg and Jim and some of you folks who've spent a lot of time in this arena to sort of help us with this part of the conversation. I see Roy is already jumping in so I'll throw it over to you Roy. Go ahead.

Roy Arends: And thanks Mikey. One of the lesser-known things about DNS is that the root servers are equipped with a file called hints, and this is basically to tell resources where the root servers are.

It's basically a bunch of IP addresses for the Root Zone, but it is a separate file and these are distributed with root server software and eventually they - it can become stale when the root server software is not upgraded.

And meanwhile the root service has moved to a new IP address; it's likely that the old IP addresses are still being queried by those resources and are being updated, so it's a little part.

It's not a big impact. If this is changed in a malicious way then all bets are off, but it's maybe a separate file from the Root Zone. Thanks.

Mikey O'Connor: Thanks Roy. Maybe we do a little brainstorming and throw out a bunch of these and then argue about whether they're in or out. Any others that people feel are kind of comparable to the Root Zone and fit into that...?

Roy Arends: Yes. Sorry, it's me again. There's yet another little known thing that's called - it's a zone file called root-service.net. And this is the zone where all the root servers are listed, and the root servers have names like A.rootservers.net and B, C and D and so on and so on.

These are actually hosted on a separate file called root-service - sorry, root-service.net which is under the Net Zone, which is again on the Root Zone. It can become a little bit - a little complex but just the same it is a separate file and I think it's an important aspect to mention. Thank you.

Mikey O'Connor: Okay, anything else or shall we stop at Root Zone hints and root-service.net? Kind of leaning towards Greg for some guidance on this. Greg you want to chime in and sort of summarize the comments that you've been making on the list?

I think they've been really helpful and I think bringing them forward, this is a good time to do that. I hate to put you on the spot but...

Greg Aaron: Yes. This is about the critical registry functions.

Mikey O'Connor: Yes.

Greg Aaron: Okay.

Mikey O'Connor: I mean, if you look at this list that we've got now, this is essentially saying that there's one - for purposes of our discussion we're really zeroed in on root and potentially ancillary files that support it like hints and root-service.net.

The question that's - that I was framing out there on the list was well, are there other things, WHOIS, EPP, and basically one of the distinctions that came to mind was the difference between the provisioning side of the DNS and the delivery side. And so, you know, I kind of lean on you especially for clarity on this and...

Greg Aaron: Okay. Well in this case it's - we need to think of the Root Zone as being separate from a TLD Zone, okay. The Root Zone telling us where each TLD is located basically, and then the Root Zones are the zones that are operated by each registry operator, okay.

What I was talking about were the critical functions of running a registry. Now one of those is provisioning information back and forth between the registry and the registrar.

Registrars put data in, they get responses back out or they query and they get data back out. So ICANN in its contracts considers that a critical function, right.

You can't really run a registry if they're not - if you're not talking with your registrars and that's how the registrars get name server and host and IP information in and out.

EPP is one way to do it but there are other ways. Then basically publishing the zone files to summarize is another critical function, okay. So the registry is facilitated for that.

It's the only place it can be done. They have to disseminate the data, okay. So that's a - that's the critical DNS function basically. DNSSEC might be considered a subset of that.

If you're going to do DNSSEC you have to do it correctly of course and do it securely, but there are some registries that don't offer DS records and all that kind of thing right now. So that's why I was saying don't list DNSSEC specifically as a must-have.

Mikey O'Connor: Right. But you'd agree that the provisioning information is a must-have, right?

Greg Aaron: The provisioning function, not the - yes, that's the function that's critical, right, so that - now again Mikey that's registrars putting data in and querying data back out. That's one function.

Mikey O'Connor: Right.

Greg Aaron: Separate but related is the registry publishing the zone files.

Mikey O'Connor: Yes, and I've got the - I'm thinking that that's what this is, the major zones, minor zones. Now are you thinking in terms of zone file access, the sidebar publishing that...?

Greg Aaron: No. Zone file access is something very different.

Mikey O'Connor: Yes. Okay.

Greg Aaron: That's a term of art so to speak.

Mikey O'Connor: Yes.

Greg Aaron: And, you know, that's just, you know, whoever wants a zone file they can acquire it and that's done in the gTLDs as a requirement, but most ccTLDs don't offer subscription.

Mikey O'Connor: Right. So if we were to - I'm thinking that I might just take the hints and root server if I could figure out how, put them in DNS critical port files, which I would like to be able to drag in but not be able to.

Oh there we go. And then treat them as one thing. Roy, is that okay if I do that?

Roy Arends: That's okay. Thanks.

Mikey O'Connor: Okay. And then we'd have one more addition, because remember this is all about configuration errors by privileged users so we'd have one more kind, which is I'm going to stay with information - well no, I - actually I could see turning that - shall we call it functions or systems Greg? I want something we can misconfigure so it fits with our...

Greg Aaron: Yes.

Mikey O'Connor: Let's call it systems for now and we can always fix it. Okay.

Greg Aaron: I think what you're talking about there Mikey is a registry secure, and that gets into the area of is a registry system secure or not? Can unauthorized parties get into it for example?

Mikey O'Connor: Well no, that's a different one. An unauthorized one is going to be in our adversarial threat sources. This is really a mistake by a user that has the privileges to do this. They just screw up and misconfigure it.

Greg Aaron: Well are you talking about a screw up by the registry operator?

Mikey O'Connor: Well either side it seems to me and this - in the provisioning...

Greg Aaron: In a provisioning system, I mean, a provisioning system is dumb in that whatever a registrar puts into it that's what it does. Now a mistake might be, "Oh I accidentally deleted the wrong - the main name."

But that would seem to fall beneath our minimum kind of a - to that level we're trying to think about.

Mikey O'Connor: Yes.

Greg Aaron: So...

Mikey O'Connor: So this is primarily provisioning - well let's narrow this to a registry administrator misconfigures. That's kind of a lame language but it kind of captures the thought, which is that this is primarily at the - well this is only at the registry, correct?

Greg Aaron: Yes, we're not talking about the root itself.

Mikey O'Connor: Right. Okay. Any others for - oh, Joerg has got his hand up. Go ahead Joerg - Joerg.

Joerg Schweiger: Yes thanks Mikey. Joerg for the transcript. Sorry, I'm not completely seem to getting it what we are talking with this last point. It may be that I'm just on the wrong track and we're going to relevant - we want to relevant it with accordance to giving it low significance by saying that the relevance is just not there.

But I would really look forward to anybody who would give me a - an example where a misconfiguration of say an EPP client could force anything that would - could really damage or harm the DNS and that's what we are talking about.

I would suppose that if a misconfiguration would take place, well in this case two things might happen. First thing, the EPP client might not get a connection to the registry's system.

It wouldn't harm the DNS. Second, we would transfer wrong information concerning a contact information or a domain information. Well, no damage for the DNS, so I'm not really figuring out why we're discussing this.

Mikey O'Connor: Well I think that what we want to do is capture this and then capture your thoughts in the discussion of...

Joerg Schweiger: Something added with relevance like...

Mikey O'Connor: Well both I think, act and relevance. You know, it may be that they're very low, but I think at the same time what we're trying to do here is document these things so that others who follow us can say, "Oh yes, that's right, there is that thing."

And then argue with us about our decisions about whether it's relevant and whether it's got a very broad range of impact. But I think it's legitimate to put it in if nothing else, then to dismiss it as a trivial or unlikely sort of thing later.

But the reason that I'm working this so hard is because I think we're going to see these threat events, this list that's opened up again and again. And I want to make sure that we've got a complete list. Jim, go ahead.

Jim Galvin: Yes thanks Mikey. I didn't want to comment on that. I wanted to say something else, so did you still want me to go?

Mikey O'Connor: Joerg, are you okay if we keep it on the list and just dismiss it in our evaluation?

Joerg Schweiger: I'm not sure whether this is going to lead us to something that is really absolutely good for the result of what we are doing, because in that case we do have to consider DNSSEC.

For example we might want to look at specific errors. We might want to look at SSL errors and so forth, so I'm just not sure whether this is going to go into the right direction or not. But I'm just going to observe and see what is going to happen.

Mikey O'Connor: Okay.

Joerg Schweiger: So go on Jim.

Mikey O'Connor: I mean, we can always, you know, it's easy to eliminate things. It's hard to reinvent them six months down the line when we go, "Oh, we should've put that in." So I'd rather have too many things than...

Joerg Schweiger: It will divert us and it makes - it's going to make a lot of work associated with it, and it's diverting us from the real stuff. And we might end up with 100 -

report of 100 pages or something like that where the really central information is just on ten slides.

Mikey O'Connor: Yes, but I think we finish that - I think we fix that later. I don't think that we're that far off track yet.

Joerg Schweiger: Okay. I'm trusting you Mikey.

Mikey O'Connor: Well thanks. Okay Jim, go ahead.

Jim Galvin: I just wanted to go back to the line item you have about - excuse me. So this is Jim Galvin for the recording. I wanted to go back to the line item critical DNS support files.

Roy had - I wondered if it might be appropriate to put a little more detail in there so we know what we're talking about. You have those two. I also added in the chat room over there talking about the resolver configuration file, because certainly that could be used maliciously to redirect forwarding in the same way that one could, you know, maliciously adjust the hints file.

And we also have a reference to the trust anchor file. It would certainly have the root's public key that is probably configured at individual resolvers. You know, those are all part of critical DNS support files and it should all be...

Mikey O'Connor: Yes I know. This is Mikey spazzing out in spades because I can't figure out why I couldn't just add it right under there. So I'm adding them where I can.

Jim Galvin: Oh okay.

Mikey O'Connor: And then I'll figure out how - what I'm doing wrong. So what was the first one that you mentioned Jim? I was so busy...

Jim Galvin: Resolver configuration files.

Mikey O'Connor: Oh no.

Jim Galvin: So we should include those in our discussion at some point when we want to get more into this. All of those things should be talked about together as we decide whether or not they're critical or not.

Mikey O'Connor: Right. Now are we thinking that all of these are similar enough that we can evaluate them in one blob, or should we split them apart and evaluate them in terms of their range of impact and their relevance? Should we do them together like this or should we do them separately?

Jim Galvin: Well I'm okay with them like this for right now but, you know, if you want to have a discussion about it let's see what other people think.

Mikey O'Connor: Yes. Yes. I mean, I'm okay putting them together, but I don't want to accidentally sweep a bunch of things into one pile that shouldn't be. So we'll leave that way for now, and then if somebody feels uncomfortable with it we'll split them apart.

Okay, any more for this sort of - again this is configuration errors by a privileged user. It will give us enough to do for the rest of the call so I'm fine stopping here, and then attempting in my lame way to put these two pieces - so far so good. This is what I don't understand, there you go. All right, so it's voting time, people. Oh, let's go back and tidy this one up. This is one I typed sort of on the fly that sort of triggered a bit of a discussion that we never finished.

So, why can't - oh, there we go, right click. What do we want to do with DNS? Jim, is that an old hand or a new hand? You want to - you or Greg want to help us out with the DNS (seg) part of this? This is again; the administrator misconfigures a threat event. Is this one that we want to leave in, leave out, (find)?

Jim Galvin: Was this added last week?

Mikey O'Conner: It snuck in a couple/three weeks ago and it was right at the end of a call and so I just typed it in as kind of a reminder to us to say, "What is this critter and what are we going to do about it?" So we could easily take it out if people want to. It just came up right at the end of the call. Greg, chime right in.

Jim Galvin: Well, I don't remember it being added. I mean, I could invent something here but if somebody remembers it being added and has something they want to say maybe we should give them a chance to speak first.

Mikey O'Conner: Yes. Greg?

Greg Aaron: It's Greg. So a major DNS provider might be somebody like buying DNS, or Google or (Ultra) DNS or (fair), who often manage DNS services. They're - in other words, not a registry operator or a route operator but somebody else who does DNS services.

And they do have, you know, a lot major customers, a lot of major Websites use them, but they - if they have some sort of a misconfiguration or problem it may only affect all to some of their particular customers. So I think the question for us is does that rise to our minimum threshold. So it seems to be more of a provider or localized problem.

Mikey O'Connor: Yes, I could live with that review. How do other people feel about that? I'm not hearing any howls of protest. We'd...

Jim Galvin: Yes, so this is, Jim. So the issue that we're driving at here is just that you have someone who serves the large community and if that provider has issues then it really just depends on what we define major as. So that becomes part of the discussion that we ultimately have to have. You're

relevant if you're major because then you affect a greater user community. Is that the point we're trying to make here?

Mikey O'Connor: Yes, I think that is part of the deal.

Greg Aaron: You know, and - well, I don't know how much of the Internet - or how many of the Websites, specifically, any one of those providers - the bigger providers serve. It's not unusual for a really big site like Amazon or Facebook or somebody to use one of these.

But is the failure of Facebook big enough? To me it doesn't seem so and even if the managed DNS provider have some sort of a problem I don't know if that site would stop resolving.

Mikey O'Connor: What about VeriSign?

Greg Aaron: They're a managed DNS provider also but only for certain customers like the others.

Mikey O'Connor: Yes, so we could even put VeriSign in our list of example providers, right?

Greg Aaron: Yes.

Mikey O'Connor: But what if they - what if VeriSign - isn't VeriSign the DNS (seg) provider for the dot com zone, too?

Greg Aaron: Those are separate services.

Mikey O'Connor: Yes.

Greg Aaron: Serving the dot coms is separate from the managed DNS services they offer, to be specific, corporate customers.

Mikey O'Connor: So should we reword this to talk about the DNS (seg) that serves a major zone?

Mark: This is Mark. I feel like compelled I need to jump in here. So with managed DNS VeriSign is a really small player in this. It's actually (Affilius) that has a much larger - no, I'm sorry, not (Affilius), it's (NewStar) that has a much larger customer set with their Ultra DNS product.

So it's a matter of what you want to - the whole idea of going major/minor starting going down to a rat hole really quickly especially when you deal with managed DNS.

Mikey O'Connor: So what if we didn't go after the providers but rather went after the DNS (seg) that supports say the dot com zone, if and when it gets - I can't remember, is dot com assigned now?

Man: Yes, it is.

Man: It is, but then don't single out dot com. I mean, then you're talking about TLDs that are assigned. I mean, you might as well speak to it more generally.

Mikey O'Connor: Right.

Man: Because now we're getting into this question that we've had before. I mean, there are certain countries that are really, really small, in the scope of the larger Internet so what if the country goes offline? In the scope of that country, I mean, it's just a huge crisis, right? And this, I think, I have to agree with Mark here. I mean, this is where this rat hole pops up.

The same thing with DNS providers in general. I think that major providers are providing services for major companies, okay? Facebook is probably a good example because different people have different opinions about whether social media is important or not. I'm sure that the 10's of millions of

Facebook users would care a great deal if Facebook went down because their DNS provider went down.

On the other hand, from the grand scheme of the Internet in general, how important is it really?

Mikey O'Connor: Yes, and I think...

Man: So I think these are tough things to document and talk about. We have to find the principles that we're trying to speak to here and not try to focus on examples, because the examples are - they're like analogies, they're never going to cover everything you want.

Mikey O'Connor: So I'm going to put two in so that we can make that distinction, and then what we can do is we can maybe give these different - so let's say that to capture that difference we have, this one, which is a provider, and then we have DNS (seg) for a zone, TLD zone. Does that capture the distinction that we're trying to make here? Then we can go off on range of impact and relevance and do our damage over there about that.

Man: Well, I guess the other distinction that came out of talking about a provider is talking about large corporations or businesses. I'm not sure what word we want to use here but I think large corporations.

Mikey O'Connor: Let's say large businesses. Does that work? It sounds close enough. This is all highly repairable. Okay, it's voting time, people. We're going to start with that one that we just talked about and we're going to vote range and relevance.

So first, and I've recruited Nathalie to be the manager of the voting so that I am not quite so lame on that. So the first thing we're going to vote on is the range of impact of a major DNS (seg) provider, and - but this is a third-party provider, not the DNS (seg) for an actual zone file.

And so go ahead and use the scale on the screen just like you're doing, you're doing fine. And we'll sort of push the pace along here for now and see if we can get done with all of these before the end of the call. We should be able to make that.

So it's looking like there's a few in the middle, sort of in the 5's zone. Oh, dagnabbit. New subzone, where's the new (child) zone? It looks like a 5 for that. I've got to figure out a keyboard shortcut for that. Going once, going twice, everybody voted? Okay, so Nathalie, you can clear the votes on that one.

Now we'll do the same thing on relevance. This is the one has it been seen, has it been seen by somebody else, has it been reported by a trusted source, is this, you know, predicted, it is possible, etcetera? So go ahead and vote on that one.

Patrick's come in, there we go. Oh, don't take my highlighting as any kind of a hint. So again, this is the one where somebody misconfigures their DNS (seg). Woo, got eight, okay. Anybody - nine, we're up to nine. Any more? Ten. Going once, going twice? Okay. Nathalie, you can clear that one. Oops. See if my - hey, would have been.

All right, so now we're doing the DNS (seg) for a TLD zone. Same questions, range of impact, sweeping to not so sweeping is the one we're on right now. So if - just to pick on VeriSign, if they - if somebody in VeriSign misconfigured the DNS (seg) for VeriSign what would the impact be? And people are starting to vote, it's sort up in the extensive wide ranging zone right now.

Man: Well, just to be clear here you're not asking us to vote specifically about VeriSign.

Mikey O'Connor: Right.

Man: You're just using that as an example for the concept, right?

Mikey O'Connor: Yes, yes. It could be (.nzed); it could be .au, anything. Okay, I see ten total. Going once, going twice? Okay, three and seven. Okay, Nathalie, we can clear that one and go on to the relevance one. Oops. Swear word. Talking about whether it's been seen all the way down to described by a credible source or not even applicable.

Eight votes, going once, going twice. Okay, we'll record that as one. Oops, not eight and two. Okay, Nathalie, you can clear out the gizmo. We'll go onto the critical DNS support files. They're listed up here and we'll do the range of impact one first, which is the scale on the left side down there on the bottom of your screen. So this is the sweeping versus not too sweeping one.

Go ahead and vote. Looks like we're getting there, looks like eights and fives is what we're producing, go three and seven. Okay, that one's done. Nathalie, you can clear the results on that and we'll do the relevance - oops, dagnabbit. There's the one where we - have we seen these files misconfigured when we get them back up on the screen again, anticipated as possible, you know, that list?

Jim Galvin: So this is Jim Galvin. It's interesting, this is probably the spot where if I were going to split those files this is where I would split them.

Mikey O'Connor: Okay. Which ones do you think (unintelligible)?

Jim Galvin: I mean, I'm not going to ask that we split them, I just - I raise that and see if anybody else jumps in and wants to do it. But otherwise, I think we leave it alone for now. There's going to be plenty of time to expand on this as we get to righting text.

Mikey O'Connor: Yes. Okay, we'll leave them together and then see if we want to split them later. It's looking pretty anticipated. Okay. Okay, we've got eight for that and one for that - two for that. Great then.

Okay, moving right along. Oops, this is the provisioning one that we just added. So again, a registry operator has misconfigured the provisioning systems between registries and registrars; EPP is one example. Range of impact, whoa, that was interesting. I bet you can't see my screen anymore. I just had one of those network fail things on my Adobe Connect session.

Sorry about that. Anyway, we're still on range of impact. Go ahead and vote on what you think the range of impact would be if registry misconfigured their EPP systems, presumably so that registrars couldn't use it. I think that's the, you know, presumably that means that registrars couldn't add or remove zones from a TLD. I'll add that to the description.

The votes are up to a total of eight, nine, ten. That's pretty close. It looks like we're in three and five zone here. So start recording that. Oops, wrong place, sorry. Oops, we're way down. I've completely screwed us up. Sorry, I have to do this all over again. But we're doing range, not relevance. There is no option for zero. So for those of you who are voting zero, can I give you a one? Can I combine the zeros and ones that you've voted?

I'm going to go ahead and do that. So four people think that it's a limited impact, and six people think it's minimal. Let's make sure that if you voted zero you're okay with that, and if it's okay we'll keep going. Sorry, I goofed up.

Okay, Nathalie, I think we can clear the poll and go onto the relevance one. Again, where we've seen it, is it something we've seen and - or is it something that's purely possible or somewhere in the middle? Up towards a total of seven, a few people still pondering. Going once, twice, we'll call that done.

All right then. I think that this might be a good spot to break because we're - unless we have more configuration errors by privileged users, we've just finished this little chunk of the work. So I think this might be a last call, now that we've sort of dug into this for other chunks of the DNS infrastructure that can be misconfigured by privileged users.

And if there aren't any then what we'll do is we'll go to work on the next big one, a business failure by a key provider, next week. But I think that's too hard to start. I have to go off and do a little research in some of the other mind maps before we start that one so I can populate a few just to get you thinking about it.

So any other thoughts, business that they want to bring forward before we close for today that otherwise we'll close a little early? Okay, I'm getting enthusiastic support from the chat. So I think we'll call it a day. Thanks, all. Nathalie, I think you can wrap up the recording and we'll see you all next week.

Man: Thanks, Mikey.

Man: Thanks, Mikey.

Man: Thanks, Mikey, bye-bye.

Man: Thanks, Mikey.

END