ICANN Dakar Meeting
Joint DNS Security and Stability Analysis Working Group TRANSCRIPTION
Sunday 23rd June 2011 at 18:15 local

Note: The following is the output of transcribing from an audio. 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.

Coordinator: This call is being recorded.

Stephane Van Gelder: Thank you, Operator. Welcome to the last session of the day for the GNSO Council. This is an update from Mikey O'Connor on the DS - the activities of the Joint DNS Security and Stability Analysis Working Group, aka DSSA. And Mikey has bravely agreed to give us that update remotely.

I'm just looking to Marika to know if the slides...

Marika Konings: Oh, yes.

Man: So Mikey, we're ready for you. Please take it away.

Mikey O'Connor: Thank you, sir and thanks Marika. It might be helpful if I could get promoted to being a presenter. That way I could turn the slides. But it's not a big deal. Here we are.

Marika Konings: And Mikey, it is Marika. The slides are now - everyone can scroll them. So everyone can move along in the Adobe Connect.

Mikey O'Connor: All right. That's fine. So I'm going to just start this off by reminding folks of our charter. You've seen this before, but especially given the great presentation that Alejandro just made, I think it's useful to contrast what our two groups are doing.

Alejandro and the SSRRT are doing a very broad review of many facets of the SSR management function in ICANN. The DN - the DSSA has a very narrow charter. We are really zeroed in on the threats and vulnerabilities of the DNS and leaving the managerial and risk assessment sorts of issues to others.

And so just to remind you, this is a collaboration between the at-large CCNSO, GNSO, GAC, NROs and SSAC.

And with that, I'm going to move on to the next slide, which is to - the goals for today, which are really to let you know what we've been doing. We've done a lot in the last several months -- bring your awarenesses up to speed a bit.

And just as Alejandro, did throw a plea your way for input on what we've got. A little housekeeping item -- hopefully there are one-page summaries of this floating around in the room somewhere. If not, if the folks who know where those are could track them down, that would be great.

We're trying to get the word out pretty broadly, especially in Dakar, on this first round of work that we've done. We're not done but we think it's pretty good and we really want your input.

So on the next page, which is called Approach and Status, this just gives you a sense of where we are. We're a project. We have a beginning, a middle and an end. We're very much in the middle right now.

We're in the stage of the work where we're identifying the threats and vulnerabilities that we are then going to go on to analyze in the next phase, and a sort of informal assessment says that we're about 70% complete, but it's still very fluid.

We're still really interested in input. We're really interested in places that we may have gotten off track or things that we've missed. And again the goal of the one-page handout is to give you the list of all 50 of us, any of whom you can contact with ideas, suggestions, course corrections, whatever.

So on to the next slide, which is called Activity Since Singapore. I'm not really going to work you through all of this stuff. I know you're all at the end of a really long day. But I do want to point out a few things.

We have made a lot of progress on these lists. We've also -- and if Alejandro's still in the room -- this is something that, at the third bullet on that first chunk, we have developed a mechanism for segregating sensitive information that might be useful to the SSRRT, and we may want to share that.

The two groups are having a joint meeting on Thursday morning. So Alejandro, just a heads-up about that one.

You can see the remaining work. I've sort of touched on that already. And now I'm on to the Brainstorming and Refining page, which - the main point of this is to show you that underneath this fairly sketchy outline that you've got in front of you, there is a lot of detail.

And that detail is available. It's updated every week on our web page in the ICANN Community Wiki. And believe you me, if you want to see a lot of detail, try printing out the web page version of this stuff. It goes to something like 60 or 70 single-space pages of bullets. So this is an extremely high level summary of what we've got. Again, we're really interested in your thoughts about that.

Next slide is called Scope. This is just a reminder of the scope discussions. The group has had a lot of discussion about scope, not unlike the SSRRT group. And this just highlights what we've declared as the limits of our scope.

It's not that the things that we are going to show you in a minute are out of scope for ICANN, but they're out of scope for us, given our charter.

Okay, so on to the meat. The first slide is called Threats to Underlying Infrastructure. And the way all three of these slides lay out is that we have highlighted the things that we are going to talk and analyze in green. We have some in the middle that are under discussion. Those are in blue. And we would be especially interested in people's thoughts about that topic.

In this particular case, the topic is the business failure of a registry. And we have not arrived at our conclusion on whether that is in or out of scope from our perspective as a threat to the DNS or TLDs. There is - there are good cases on each side of that discussion.

And we've - on this first page we have one that's out of scope. We're not going to take a look at the depletion of IPD4 address space, primarily because this is going to happen no matter what and it's not necessarily something that's really going to impact the DNS a lot.

But again, we're really interested in your reactions to our rationales -- to things when we took them out of scope. So if there are disagreements, refinements, et cetera, we really want to hear about those.

On the next page, Threats Which are Direct Attacks. We have a series, again, that we feel are in scope -- distributed denial of service, pack and intercept, et cetera.

We have two that we're still discussing. The first is IDN attacks where lookalike characters are really used for standard exploitations. And we've decided to wait until the variance projects are a little bit further along before we decide about that one.

And the other is Malicious or Unintentional Alteration of DNS Configuration. That one's pretty esoteric inside baseball. But again, if any of you are interested in this, we'd love to hear from you.

And then in the out of scope are things like footprinting, which is essentially an attacker scanning DNS entries to try and build a footprint of infrastructure, authenticated denial of domain names, malicious or unintentional alteration of contact information. This is really more on the second level or, in our view, are considered threat factors rather than actual direct attacks.

And then the final one in the threats work that we've done is in what we are calling indirect attacks. And we have one really esoteric one that popped up because of the possibility of email server hopping under IPv6, which may cause a certain amount of collateral damage, as the hopping across a lot of addresses causes a load issue.

So we're going to take a look at that. But you can see a long list of things that we are not going to consider. And it's primarily because these are - it's not that these are out of - in or out of scope for ICANN -- again, that's Alejandro's group's work to try and figure that out, what the boundaries of that are. But they are outside the scope of what we consider our charter to be, for the reasons that we list below.

And again, we're very interested in hearing from you about this because this is draft. All of this is still open to discussion, change, et cetera.

And then the final really meaty page is we've also developed a very board list of vulnerabilities that we're going to take a look at. And they range from sort of the technical at the top of the page, to the managerial at the bottom. And the one in the middle, Registry Failure and Continuity, which, in a way, relates to business failure of the registry.

We consider registry failure and continuity to be in scope for us. And the reason it's in the middle of this page is because it has both operational and managerial issues associated with it.

So that's what I've got. The last page is just the mandatory question page. And with that, Stephane, I'll hand the gavel back to you to take questions.

Stephane Van Gelder: Thank you. Thanks very much for doing that remotely. That deserves a double thank you, I think.

Are there any questions or comments for Mikey at this stage? Jeff Neuman.

Jeff Neuman: Hey Mikey, thanks for doing this. This is Jeff Neuman. You know, I think a lot of people in this - in the ICANN community, when they think of DNS, they think only of TLDDNS, and of course, at the roots. What they don't thing about is - are recursive servers or enterprise DNS or DNS at the - that's provided by ISPs or any of that stuff.

To what extent are your - how you reached out to ISPs or DNS providers for their participation to help our out in your work? I know they're not within the ICANN - some of them are not within the ICANN structure, but to the extent you talk about DDoS attacks, most DDoS attacks are not at the TLD layer. Most of them are at recursive servers or at enterprise.

And so I think it's important if you do come out with a report talking about TLDDNS that you make it clear that you're not talking about,

necessarily, denial search attacks at other layers which are probably -- not probably, but are definitely much more common than at the TLD level.

Mikey O'Connor: Thanks Jeff. You're absolutely right. Most of the DDoS attacks that take place are outside the scope of what we're looking at.

We are actively always looking for more participants. And your suggestion to reach out to some of the DNS providers and some of the enterprise DNS folks is a good one.

We're doing that this week. But the types of DDoS attacks that we are going to be looking at are primarily aimed at either the root or at TLD servers -- not all the rest.

We - we've had a pretty good discussion in the group that draws a pretty bright line between what we're working on and that much, much, much boarder scope, which is certainly a security and stability issue, but it's not a security and stability of the DNS issue, in our view.

Jeff Neuman: Yes, I just think that there's a lot of confusion as to what DNS truly means, especially in this - in the ICANN world. And I hear governments and I hear a lot of other people talk about the DNS. And, you know, most DNS services have nothing to do with ICANN or not anywhere in the ICANN world.

And so when people talk about solving issues - threats against the DNS, there's almost two DNSs. There's the ICANN DNS and then there's everything else. And unfortunately, everything else is much larger than ICANN.

And, you know, I understand it's not within the scope. I'm just afraid of people taking a report from you guys -- as you know, we solved this issue, or here's our recommendations -- and thinking that that's going to go anywhere other than solving a limited set of, as you said, the DDoS attacks or things like that.

Mikey O'Connor: Yes. But, you know, I'm back on the scope slide. The - one of the discussions we had is when we were talking - when this was more a discussion of DNSSEC than it was DDoS. But it - we started getting into a conversation about the impact of DNSSEC on end user routers -- not even ISP routers, but the actual broadband routers in businesses and individuals' homes.

And that's sort of the opposite end of this continuum. And our focus is strictly zeroed in on the root and top level domains, period. And we will certainly make that clear in the report.

Jeff Neuman: Thanks Mikey.

Stephane Van Gelder: Thanks Mikey. Any further comments?

William Manning: We'll try this one, instead. Mikey, this is William Manning. And one of the things that is a response to the attacks and the threats to the DNS, as pointed out particularly in the second bullet the - in the blue -- Threats to the System and Relevant to ICANN's Role -- a lot of response to the - these threats is to stand up what are called reputation systems.

Is this query or this thing coming from a reliable source? And what that actually involves is interception of and interpretation of DNS requests by an intermediate party, not from the authoritative source.

And this is becoming a common idea. Unfortunately, reputation systems in the DNS -- the RPZ system as published by Inter - the ISC folks -- is incompatible with DNSSEC.

And so at a very high level, the threat posed by deployment of RPZ as a way to mitigate the threat, destroys any of the efficacy of DNSSEC, and it would be maybe not part of DSSA, but this is going to come out in the SSR as a high level concern.

Do we do reputation systems or do we do DNSSEC? Because we can't do both.

Man: Wow, that's a good one.

Mikey O'Connor: One of the things that's in our charter is we are charged with doing this analysis, and only conditionally charged with coming up with ideas in terms of fixing things. Our charge is mostly aimed at a snapshot of the current state of affairs, and identifying gaps. And if there are gaps, then it's at the third level that we're charged with actually coming up with ideas.

But certainly the RPZ versus DNSSEC discussion is one that should find its way into our report too, as we go along. So I've copied that one down (unintelligible).

Stephane Van Gelder: So we have three minutes left and two people in the tube. Alejandro, did you want to ask a question?

Alejandro Pisanty: I'll be very brief. I just want to offer and guarantee the cooperation between our groups. There's overlapping scopes, and we're trying to make sure that we work together as well as possible.

Mikey O'Connor: And I'll second that.

Jim Galvin: Thank you. This is Jim Galvin. I'm Vice Chair of the SSACs. And I guess - and this will speaking here. Three minutes left. So the only that I'll say is I don't agree that you have to choose between RPV and DNSSEC. I think that's an interesting discussion to have.

I just want to go on record as stating that. And I guess we'll take that offline in the interest of time.

Man: Okay, I did ask the question of Paul (Zexy) and he said they are incompatible, and he doesn't know how to fix that. So that was a statement he made in a public meeting last week. So I - we can discuss it.

Stephane Van Gelder: Okay, thanks to everyone. Thanks to Mikey for participating remotely, once again. This brings our GNSO sessions to a close for today. It's been a long day. Thanks to you all for participating and staying with us this long. And we will, as far as the GNSO Council is concerned, reconvene tomorrow for our joint meeting with the CCNSO.

And with that, thank you very much and enjoy your evening everybody.

Operator, this session is now closed.

END