Fast Flux PDP WG Teleconference
TRANSCRIPTION
Friday 16 January 2009 16:00 UTC

Note: The following is the output of transcribing from an audio recording of the Fast Flux PDP WG teleconference on Friday 16 January 2009, at 16:00 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-ff-20090116.mp3
http://gnso.icann.org/calendar/#jan

Present for the teleconference:
Avri Doria - NCA, GNSO Council chair, Interim chair Greg Aaron - Afilias Ry c.
Paul Diaz - Networksolutions RRc
James Bladel - GodaddyRRc
Adam Palmer - PIR Ry c.
Mike Rodenbaugh - CBUC

Observers - (no constituency affiliation)
Joe St. Sauver
Martin Hall
Jose Nazario
Randall Vaughn

Staff:
Marika Konings
Glen de Saint Gery

Absent - apologies
Dave Piscitello
Rod Rasmussen

Avri Doria: I think the initial report's really looking good. Let's hope for this (unintelligible) recording, correct?

Coordinator: Madam, the recording has now started. Thank you.

Avri Doria: Okay. Thank you.

Glen DeSaintgery: If I do the roll call to save your voice, Avri?

Avri Doria: Oh please do. Thank you. You do it all the time anyway. But thank you.

Glen DeSaintgery: We've got on the call Joe St. Sauver, Avri Doria, James Bladel, Paul Diaz, Martin Hall, Jose Nazario , Adam Palmer, Mike Rodenbaugh and for staff we have Marika Konings and myself, Glen. And we have apologies from Rod Rasmussen who is not able to join us because he's traveling today.

Avri Doria: Okay. Great. Thanks. Then I'll try to keep my talking to a minimum if I can so that I don't worry people too much with my voice. We've got a draft of the report which I think is looking quite nice. But we do have some new text in there that we need to go over. And we also have two e-mails with issues -- one from Joe and one from Martin we need to cover.

And then there were some other that perhaps -- things throughout the document that we need to touch on. Let me touch -- so anything else that you know of that needs to be singled out at the moment? And of course I want to catch some people what else you may or may not have that needs to be touched on.

Marika Konings: There's some changes that are incorporated in the executive summary that were circulated to the list (unintelligible) by Greg. There was no comment on that. But I highlighted them here in track changes just in case people wanted you...

Avri Doria: Yes. No (unintelligible).

Marika Konings: ...to repeat them in more detail.

Avri Doria: And then as I said we have the promise from Joe and the comments from Martin.

Marika Konings: Yes. And then we have as well added in Chapter 6 that were done by a small group I think with...

Avri Doria: Right.

Marika Konings: ...Mike, James and Greg if I'm not mistaken.

Avri Doria: Thought I had that. Okay. Well if there's no issues, then why don't we walk through the changed places and then go through the two e-mails if we haven't hit some issues along the way. Does that seem a reasonable approach?

Man: Yes.

Woman: Yes.

Avri Doria: Okay. And so I'll go looking for the changes. The first one I have is that 83-84. And if I happen to miss any while I'm going through, please shout. And if there happens to be anything in a section before that that you really wanted to fly other than what's in the e-mails, please flag it.

Now on 83-84 we have the group that (Russell) tasked to obtain expert opinions, and appropriate on which areas of fast flux are in scope and out of scope for GNSO policy making. It doesn't seem there's any issue with that being in there, is there? Okay. Then I'll move on. And then Marika has (unintelligible). Okay. (Linda), if you happen to know where the next one is before I get to it do, you know, let me know.

The next one I have is a deletion 129-131. Whether it was a supported statement, there was reference of fraudulently created IE use and stolen identities for payment and other. That was removed and we're have just the poor quality who is. Any issue with dropping that support? Will someone remind me why we're dropping support?

Marika Konings: This is Marika. I think the reason was because this is summary. And there was no need to include the further details in there, especially because there's no need of support...

Avri Doria: Okay. Thanks.

Marika Konings: ...statement.

Avri Doria: Anybody have issue with that? Okay fine. Move on.

Man: Greg Aaron joined.

Avri Doria: Hi, Greg.

Greg Aaron: Hello.

Avri Doria: Welcome to yourself and (Alan Flowers). The next one was 142. Basically we're going through the changes at the moment -- 142. When used by criminals the name (unintelligible). I don't know why I am reading things out loud. It's probably not a good idea.

Main goals have (unintelligible) taking longer period of time during which the attack (unintelligible) be effective. It is not an attack itself. It is a way for an attacker to avoid detection and frustrate the response to the attack. Issues? None? We'll move on. Marika, can I ask you to read them when we get to the point because if I keep reading this, it will be ridiculous.

Marika Konings: Okay.

Avri Doria: All right. I'm sorry but...

Joe St. Sauver: One question before we go on. I'm seeing line numbers that differ from the line numbers you're mentioning, like I'm at 137 for the one you just mentioned.

Avri Doria: (Unintelligible)...

Joe St. Sauver: Is there a different version of the draft?

Avri Doria: ...people. I'm looking at the doc in -- up in Office. So that may have done things funny. Now I could look perhaps at the PDF. That might make a difference.

Joe St. Sauver: That's okay. I was just wondering if there was a different version (unintelligible) numbers.

Avri Doria: Am I the only other one seeing -- am I seeing different numbers from everybody?

Marika Konings: Yes. Others from me as well.

Avri Doria: Okay. Let me get the PDF if that's numbered. And I'll have to download it. I don't have -- I only downloaded (unintelligible). That's an odd sound. Yes. I forgot it.

Marika Konings: Are you ready? You want me to go to the next one?

Avri Doria: Yes, if you can. And I'll catch up.

Marika Konings: Okay. The next one is in line 274 where it's -- figures there's a correction because it was badly written before. But it now reads, "One source of best practices for protection from fast flux can be found in the phishing world. The anti-phishing working group has recently released," and so on. This is really a correction. Does anyone have any issues with that? That's a no.

The next one I have is on line 284. And it reads, "Obtain expert opinion appropriate on which areas of fast flux are in scope and out of scope for our GNSO policy making. Some members of the working group provided reasons as to why policy development to address fast flux is outside the scope of ICANN treatment while others disagreed. The working groups' fact finding and work on definitions documented how fast flux involved the main end use issues rather than domain name registration issues."

Avri Doria: Okay. Yes. I'm caught up for the night. But thank you for waiting. It's better than nothing. Is that okay with everyone? Anyone object to that? Hey great.

Man: I'm still trying to download this version of the report just so you know.

Avri Doria: Oh yes. I just downloaded the PDF. It runs fairly quickly for me.

Marika Konings: Yes. I have to apologize especially the Word version is very big, maybe because of the graphs that have been added now in the later annex.

Man: Oh. Okay.

Avri Doria: I have one question on something and I just remembered it (unintelligible). Has there not been a (unintelligible) 419? And then I understand why that's there. But please note the following content is based on and in some case taken verbatim from a description, and does not reflect the opinion of the working group on the issue.

Now that makes it a very strong statement which I'm not sure the working group intends, which is to basically say, "You don't support what's in it" as opposed to saying "and does not necessarily reflect or should not be taken to reflect an opinion one way or another." But by saying it's this way -- and I don't know if that was the intent, it can be as, "You guys don't agree with it at all.

Man: I think perhaps "may not" as opposed to "does not" would be...

Avri Doria: "May not" would be fine, too. Yes. Does anyone object to changing that one to that one to "may not?" And I think there's one other similar case later on I noticed when I was reading.

Man: I'm sorry. What line number are we at now?

Avri Doria: I'm at 419-421 -- how to assess flux. It's a (unintelligible)...

Man: Right.

Avri Doria: ...maybe at the beginning, so in italics. And I'm just worried about someone taking the strong sense of "does not reflect the opinion."

Man: Okay. I agree. "May not" is good.

Avri Doria: Okay. Then another one above it that's right at 406. That was the first one. Again, the (unintelligible) issues report and may not -- no. I'll just leave that loose. And I'm still looking for the next change. In Chapter 4 now, don't know if I missed any in Chapter 4.

I have one question on the members of the working group. Why do some of the (unintelligible) our ICANN wiki link to another so that -- because the others don't have an ICANN wiki link, don't want it? I was just curious about that and why there was a linking to that as opposed to perhaps the SOI statement for everyone.

Man: The what? The statement of interest?

Avri Doria: Right. In other words, there's one linkage or something -- why are we linking to ICANN wiki if we're linking to something perhaps should we link to the statement of interest? And that just makes it actually more useful. But that's the question.

Man: I agree with you, Avri.

Marika Konings: And the reason why it's probably in there it was like this I think on the wiki page. And I think it's probably copied and pasted it from there. And that's why those links are there.

Avri Doria: Okay. What would people think that either removing the ICANN wiki links and putting in the links to the SOIs, which should be one for everyone? And then that part is also done. Does that make sense to people? Does anybody object to that including you, Marika? You're the one that would have to do it.

Marika Konings: No. They're fine. I presume that they're easy to find, Glen?

Avri Doria: Yes, Glen?

Glen DeSaintgery: Sorry. Just say that again -- which what is easy to find?

Avri Doria: Page 540, we have the members of the working group.

Glen DeSaintgery: Yes, yes, yes, yes, yes. Thank you.

Avri Doria: I'd like to have the names linked to their SOI.

Glen DeSaintgery: They are already.

Avri Doria: In that table in the document?

Glen DeSaintgery: (Unintelligible)

Marika Konings: Some of them are. We haven't done it for all of them.

Avri Doria: Oh. Okay. (Unintelligible)

Glen DeSaintgery: There's a link that can be put in.

Avri Doria: Okay. So if that could be done I think that would be useful.

Glen DeSaintgery: Okay. Yes. The link it can be put in.

Avri Doria: Okay.

Glen DeSaintgery: It's on the Web site.

Avri Doria: Okay. Thank you.

Marika Konings: But we probably can have it -- a link on the top because I guess it's in groups, all the statements of interest together, is that correct, Glen?

Glen DeSaintgery: That's right. I'll send it to you right now, Marika.

Marika Konings: Okay. Perfect. So that'll make my life easier as well so we just have one link and then...

Glen DeSaintgery: And then we move the other one.

Marika Konings: Yes. Okay. We'll link them.

Avri Doria: Thank you. Continuing to go through.

Marika Konings: The next one that I have is on Page 45 -- the footnote there.

Avri Doria: Ah yes. I do also. It's okay. So there was nothing in...

Marika Konings: I didn't see anything before but...

Avri Doria: Right.

Marika Konings: ...I missed something.

Avri Doria: I'm up to Page 26. There's nothing in five. So we might as well just continue looking. I must say this is really very quick to complete actually.

Marika Konings: Would you like me to read it?

Avri Doria: Oh yes. I just caught that. Ah please. I think it's a good idea to read it.

Marika Konings: So it's a big deal footnote that follows from "the various TLDs are differently situated and have different needs a approaches in this area," which is now followed by the footnote which has been changed here.

Related to policies, our purpose of the recent GNSO issues report and registration abuse policies was to identify and describe various provisions, in a representative sampling gTLD registration agreements which relate to contracting parties and/or registrants right and obligations with respect to abuse.

The report found that among the gTLDs, research found that 11 out 16 gTLDs have provisions in place that address 7 of 11 or potentially could address 4 of 11 abuse. Many ccTLDs also have policies against criminal and/or abusive uses of domain names with .de and .uk being but two examples.

Related to needs, various studies have demonstrated that amount and types of abuses vary greatly from TLD to TLD, and that some TLDs do not prefer certain types of abusive domain uses at all. For example, see the dated annex to this FF working group report by Arbor Networks and Karmasphere. The anti-phishing working groups, global phishing survey domain use and trends in one age to file a late report and your build of calm TLD statistics.

Avri Doria: Okay. And that's basically that paragraph that we had in there that whether it was objection to (A and B)s of the -- that can be - had been in the middle of the text. And I think it's good footnotes. Is anyone uncomfortable with it as it currently stands? So there are no objections to leaving that footnote as it is? Okay. Thank you. Next -- and thank you for reading it.

Marika Konings: Actually no problem.

Avri Doria: Okay. The next one I have is 1461, an exchange from "leaded the working group quickly concluded that" to "however, some members of the working group expressed that." Any objections to the change? Lower there was just a smaller correction (unintelligible) at FF servers. It may be five. I'm looking at the correct stuff right now. There was a whole bunch of changes.

Marika Konings: Especially deletions.

Avri Doria: Yes.

Marika Konings: Did it come up in your version?

Avri Doria: It come up on the PDF.

Marika Konings: Okay. Good. Would you like me to read them?

Avri Doria: Yes. And this is the work that was done by Mike and others, correct?

Marika Konings: Correct.

Avri Doria: All right.

Marika Konings: Among 1485, the following has been deleted -- "However, the members do not agree as to whether ICANN is the best organization to conduct this activity." This point is expanded on in the next section of the report.

Avri Doria: Any objections? Okay.

Marika Konings: Then in line 1489, the following is deleted -- "The question was asked whether a PDP was started prematurely. The March 2008 issues report had already recommended that further fact finding and research would be helpful in order to inform the community's deliberations."

Avri Doria: Now I'm wondering actually at this point whether necessarily reading all the deletions in next section. Anybody object to that deletion? Okay. Then I'm wondering whether a delete -- reading of all the deletions and additions in this one will be helpful or whether it's worth just reading through the new text, and seeing if people are comfortable with that since that was a, you know, sort of single piece of work of rewriting the text by deleting major chunks and reordering things, restructuring.

So I suggest just reading that section. In other words, then do the -- and I can do it or Marika, if you would just read through or perhaps Mike who's contributed could read through and just make sure that it sounds right to people. Anybody?

Marika Konings: I'm happy to read it.

Avri Doria: Okay. Thanks.

Marika Konings: So this is on 1419 -- issues with the charter. Neither the GNSO council nor the charter identified what objection of a potential recommendation on fast flux should be. Also, the council thought it saw a structured fact finding effort examine the issues of fast flux beyond the staff offered issues report.

But because no such mechanism currently exists, this effort was conducted in the context of the PDP. As a result, some felt that the charter did not provide sufficient information on what was expected to be delivered by the working group nor were important questions included.

The group struggled with finding the right balance between respecting the charter, the lack of information and the need to find a solution and consensus. In its upcoming revision of the PDP, the GNSO should include an orientation of working group members as an early step for every group to familiarize participants with the PDP process.

Some members of the working group offered reasons why policy development to address fast flux is outside the scope of ICANN treatment. Others disagreed. As some participants pointed out, some of the discussions and proposed actions might be more appropriate for other professional or community bodies, that deal with security and Internet abuse issues.

Avri Doria: All right. I like it. It’s clean, fairly neutral writing. But anybody object to that rewrite? Okay. Thanks. Great job on doing that. I think that gets it said. And it is I believe fairly neutral. Okay. Thank you. Okay. Moving on.

Marika Konings: I think the next thing is the data annex.

Avri Doria: Before we move on to the data annex and issues with that, I’d like to if it’s okay go back and deal with the issue -- Joe’s issues. Yes. Because they’re in the section of the document, and once we get through with these we’re I think done with the main body of the document. So Joe, would you like to walk us through your issues?

Joe St. Sauver: Sure. So essentially if you go ahead and look at the copy of the message I sent out. You know, one of the issues was just essentially a typo. I think there was an “and” that should have been an “an” on line 49. And likewise there was another typo on 103 that should probably read, “without notice to or consent of.”

Avri Doria: If we are...

Joe St. Sauver: And I think you indicated, Marika, you were okay with those, too?

Marika Konings: Yes. No problem.

Joe St. Sauver: And then the one I think that is probably more substantive -- although again it's just a matter of working more than anything else -- was around line 109. It talks about rapid modification of IP addresses for malicious content hosts. And if I were reading that, it would sound almost as if the IP addresses of the individual hosts are being changed. And that's not really what's happening.

What's really happening is is the fast fluxing network is selecting different hosts. The IP addresses of the hosts themselves are static. But the set of hosts that are selected to be part of the fast flux network goes ahead and changes. And, you know, I think that's just sort of again a matter wording rather than a substantive change. But, you know, I understand you're less comfortable making that change, Marika. Is that true?

Avri Doria: Yes.

Marika Konings: Well my concern was that the parts in the executive summary are taken from throughout the rest of the document. So I just want to make sure like if we make the change here, it should also be addressed...

Avri Doria: Okay. Where...

Marika Konings: ...in the other parts right up here is all we need to go back to the other parts to see if there additional information there that, you know, is okay or explains it in further detail. And it only needs to be changed in the executive summary.

Avri Doria: Did you...

Man: So what Joe is saying now on...

Avri Doria: (Unintelligible) places?

Joe St. Sauver: I did actually. So line 109 is in the summary. And line 568 in the PDF dates 12 January is where the other part of that is quoted from.

Avri Doria: I see. So it would need to be changed. Does everyone agree with our change?

Man: What would the change be to?

Avri Doria: Yes. That's why I corrected myself.

Man: I agree with Joe that it is confusing and misleading as written.

Avri Doria: Would replacing the word "modification" with "switching" -- or is there a better word -- whichever?

Man: I don't think it's just that single word.

Joe St. Sauver: I think just the sense of the sentence needs to be changed. I mean I'm not passionate enough about it to go ahead and try and, you know, wordsmith it in any great detail. I trust Marika or whoever to go ahead and do that.

Avri Doria: We should probably resolve it now because I don't see us needing to come back again. So if we can avoid coming back it again on this document so that we can call it done at the end of this meeting, I'd be really happy even if we have take one more look at it. I'd really like to finish things if we can to come up with the change.

Man: I agree with that. What line item -- what line number is it again? Say it again?

Avri Doria: We're at 109 and 568. There were two instances.

Man: 109.

Man: Joe, should we use maybe the word "rotation?"

Joe St. Sauver: "Rotation" would work fine. I think the one consideration there is that it might go ahead and never rotate back if you get my drift. When I think rotation, I think maybe half a dozen hosts and it's cycling among them. But it might just continually go through a series of different ones.

Avri Doria: Yes. That's what I was thinking of.

Man: Yes. Okay. Or "change" or "switching" or something like that?

Joe St. Sauver: Sure. Something along that line.

Avri Doria: Maybe critiquing of IP addresses is done in several contexts. This one happens to be, you know, one of our general contacts. But talking about switching IP addresses is not an abnormal concept.

Joe St. Sauver: No. And I mean somehow this actually will go ahead and do that kind of behavior in other situations.

Avri Doria: And there's a whole technology on label switching which is switching IP addresses. So it's a common problem.

Man: Joe, if we included server target in front of IP addresses, would that help point the -- be more descriptive that the underlying servers were being changed as opposed to the IP address of the single server?

Joe St. Sauver: Sure. Yes. I'm open like I say to pretty much any wording that would kind of get to that end.

Avri Doria: So would you collect that modification of server target IP addresses? Would that be an acceptable change to people? Any objections to changing those two instances to modification of server target IP address?

Joe St. Sauver: It does kind of wonder whether that actually going to capture the idea...

Avri Doria: Yes. People should...

Joe St. Sauver: ...that you're really selecting...

Avri Doria: ...still decide.

Joe St. Sauver: ...different hosts.

Avri Doria: I'd say if you're happy -- how about if we combine them all to "switching among server target IP addresses?" Does that then get it? Then it is kind of obvious I think. Does that work for people, "switching among multiple target IP addresses?"

Joe St. Sauver: I'm fine with whatever the group wants to do.

Avri Doria: Is that an acceptable change? Does anybody disapprove of that change?

Man: Could you repeat that sentence in full one more time, please?

Avri Doria: Oh yes.

Man: I just want to...

Avri Doria: Yes.

Man: ...hear and think about it.

Avri Doria: "Switching among multiple target IP addresses for malicious content hosts, main servers and other network components (unintelligible) entries with low TTLs."

Man: I guess the key thing for me is just the emphasis on the fact that it's different machines rather than different IP addresses. The IP addresses are going to be different because they're different machines. But the machines aren't going to go ahead and be reconfiguring to new IP addresses.

Joe St. Sauver: Yes. I apologize for not catching this earlier. I should have gone in and caught it on the original main body of the text.

Avri Doria: That is the latest wording. I tried not to lay that to you. Or can you still imagine that we're still talking about a single box?

Joe St. Sauver: Not necessarily a single box. But I could see somebody thinking that, "Oh. The thing goes ahead and changes between machines. And the machines may even have their IP addresses changed. Maybe it like re-DHCPs or something like that." I don't know.

But essentially the idea is if the thing goes ahead and selects, you know, candidates from this pool of botted hosts and it goes ahead and takes those candidates (unintelligible) or bridge them into its network.

Avri Doria: Okay. So in other words you're saying it really does need a restructuring because it's modification of the DNS entry is what you're really talking about?

Joe St. Sauver: Well the DNS entry is more a means to an end. I mean the DNS entry points at the botted host that it has chosen to use at that time.

Man: Yes. But it's the DNS...

Man: Change.

Avri Doria: Right. How about keep trying? I mean I usually hate wordsmithing online. But I think in this case it's worth the effort. I think it was "modification of DNS entries with low TTL among multiple IP addresses for malicious content hosts, names, servers and other network components."

Man: That sounds closer I think.

Joe St. Sauver: Yes. It is an A record modification.

Avri Doria: And so at that point you know that your changing the DNS entry.

Joe St. Sauver: Right. They actually select IP addresses with infected hosts as candidate A -- as IP addresses for the A records.

Avri Doria: Yes. Now I understand what's being said.

Joe St. Sauver: Yes. It's tough to say. I like the switching.

Avri Doria: Well right. Anytime we put IP addresses in the lead in a sentence, we leave open the option that it's not multiple hosts or that it's one host with multiple addresses.

Joe St. Sauver: Yes.

Avri Doria: And that really the problem of the way it's structured.

Man: I'm here to say selection of botted hosts for use as malicious content hosting, name servers, other network components, blah, blah, blah.

Avri Doria: Try the beginning of that again.

Man: Selection of botted hosts for use as malicious content hosting servers, name servers and other network components via, blah, blah, blah.

Avri Doria: (Unintelligible) I missed the word you said before hosts. I'm sorry.

Man: Botted.

Joe St. Sauver: Botted. Yes.

Man: B-O-T-T-E-D.

Man: Sorry about the background noise on my line.

Avri Doria: Does that work for people? There any objections even that (unintelligible)? Marika, have you captured and could you...

Marika Konings: No, not completely. Joe, would you mind sending it maybe to me in an e-mail the exact language to make sure I get it right?

Joe St. Sauver: I'll send it out to the list if you like.

Marika Konings: Thanks.

Avri Doria: Okay. Then we'll come back to it at the end of the meeting if you've all received this just to make sure. Okay. Then let's go to the next -- do when (Charles) left because (Charles) may be doing to things at the same time.

Joe St. Sauver: Let me just stay with this one for another few seconds...

Avri Doria: Okay.

Joe St. Sauver: ...or so. So the next one essentially was just that line 145 talking about how that section appears to be sort of redundant with respect to lines

185 to 193. And I think 185 to 193 probably do a better job than 145 and the following does.

Avri Doria: You think it does harm being redundant?

Marika Konings: But again this is just a summary of what is in the report and basically addressing -- because there are different -- the highlighted ones or the bolded ones are the charter questions. So if we would leave that out it means we haven't -- the executive summary wouldn't reflect that we've answered that question.

Avri Doria: Okay. So it's not really redundant to take back in a summary.

Joe St. Sauver: I guess my suggestion that would be making it parallel both in the body of the text and in the summary, so that it kind of follows with the same set of, you know, items in 185-193 and at 145 because it really does kind of rehash the same group. It just doesn't do so completely in the 145 case.

Avri Doria: Are you saying it's not -- not that it's redundant bothers you but that it's different?

Joe St. Sauver: Correct.

Avri Doria: What do other people think? It's certainly not that long a section to not include it. What do you think, Marika? You have any objection to just bringing 185 through 193 and repeating it where you have 145 through whatever?

Marika Konings: I'm happy to take another sentence from the section of the report on the, you know, benefits from fast flux to describe these organizations or the content that's switching to add a sentence there. Is that what you would like to do? Do I understand correctly?

Avri Doria: I think if I understood what basically was being looked for is to actually repeat the content of 185-193 in the executive summary.

Joe St. Sauver: Well 185-193 is part of the executive summary. It's just in a different section of it.

Avri Doria: Right. That's right.

Joe St. Sauver: The problem just is that they kind of just, you know, have a little bit more than the other one does.

Avri Doria: (Unintelligible)

Joe St. Sauver: I'm not passionate on this one again. If folks just want to leave it the way it is, I mean I'm willing to go along just to make progress.

Avri Doria: Actually why is it repeated? It's for charter questions and benefits from fast flux and then it's who benefits from the use of that block technique.

Marika Konings: We're just looking back myself as well to see...

Avri Doria: I think maybe that the first one could be dropped.

Marika Konings: Well actually the first one comes -- the question should be there who benefits from fast flux and who is harmed. So those two questions are part of that. So maybe I should just change the headings basically to reflect that that's that one.

Maybe it makes it easier if I number the questions so people see what the questions are and these are actually subheadings within that question. So maybe that's why it's confusing and seems a duplication while it's actually answer to different...

Avri Doria: Oh that's right. That's a high...

Marika Konings: ...question.

Avri Doria: ...level question. And that comes to the other questions.

Marika Konings: So maybe that will make it easier if I basically number the questions, and then it becomes easier as well to see what are actually subheadings within those questions. Would that make sense?

Avri Doria: To me...

Joe St. Sauver: I think that would help.

Avri Doria: What do all the people react? Or do you need to see it?

Joe St. Sauver: I think that would help.

Avri Doria: Okay. Yes. That'll need to be done. So that's something that we won't finish today at this meeting. So what we'll have to do is get another report out and then just have a couple day last call on the final version of the document just to make sure it's okay. That's why I don't want to have to wait until we can schedule another meeting to call it done.

Okay. Moving on -- 156-15 (unintelligible). Working group did not reach consensus concerning the separately identical culpability of (unintelligible) hosting with respect to the harm caused by malicious behavior. I always recognize the way in which fast flux techniques were used along an attack. And you said you didn't understand the sect. Is that the issue? (Unintelligible)

Joe St. Sauver: I feel like the line numbers are encrypted somehow. And I worry I'm looking at the wrong piece here. I may need to take a second and make sure I'm on the right line.

Man: Could you repeat the line number once again, Avri?

Avri Doria: (Unintelligible) It was 156-158.

Man: Thank you.

Avri Doria: That basically sounds to me like it's (unintelligible), you know. There was disagreement on whether we wanted to blame fast flux per se for the harm caused by malicious behavior. But there was recognition that the technique did contribute and were used for bad behavior.

Joe St. Sauver: I think it might just be a line number drift moment. So for example if you look at 159 to 161...

Avri Doria: In 159 I have blank. 160 is the beginning of a section.

Joe St. Sauver: Okay, because the one I'm looking at is "the working group did not reach consensus concerning the separately identifiable..."

Avri Doria: Yes.

Joe St. Sauver: "...culpa..."

Avri Doria: That's the one I just read.

Joe St. Sauver: Great. Sorry about that.

Avri Doria: And that's it as I said. It's basically to reach separately identifiable culpability is a -- it's basically who's to blame when these attacks block hosting itself as a separate blame, as opposed to fast flux has been used by malicious behavior type. And so -- and basically from what I understand that is indeed, you know, you guys didn't say fast flux is bad. It's fast flux in some cases is used for bad but maybe, you know, and then it was a more complicated issue.

But you didn't come to a strict separate culpability determination. And then that seems to be -- unless someone wants to read the different (unintelligible) what that sentence say, is that there's no consensus in this working group that fast flux is bad separately identifiable culpability. It is bad in and of itself. And that is not a consensus. No, it was really (unintelligible).

But likewise I don't think that the group that brought all will reach -- that wanted to reach the consensus that, you know, fast flux is in itself totally not culpable. And so it's the culpability argument was a nonconsensus argument, has a separate culpability for just fast flux in and of itself.

And that's what that first history is saying to me and the person that didn't write it. Does that make sense to people? And does it seem accurate to people? Is anyone uncomfortable with that still? Joe, are you okay with it?

Joe St. Sauver: I can live with it.

Avri Doria: Great. Thank you. Anyone else? Next one -- line 187. Your content distribution network just has flux nodes hosted on systems used without the consent of their owners. I think not. Likewise (unintelligible) and they confuse systems without the consent of their owners.

Joe St. Sauver: And this essentially comes back to the point that we had clarified the fact that the sort of malicious fast flux hosting we're talking about, an integral component of that is the fact that it's done on hosts without the consent of the owner or operator of a host. So if we assume that indeed is the case, then we have issues talking about it in these contexts because they don't steal the service from folks.

Marika Konings: But as fixing goes again back to another part of the report where we talk as well about who benefits from the use as well, not in a malicious way. And that's why we've described as well as content distribution networks. So if we would make changes here, we probably need to look at the...

Avri Doria: Yes, because this section does not imply that the people that get benefits from it are good or bad, nor that they're using it successfully or not successfully. Is that correct? I mean that's how I read it, that some of the benefits -- it was some of the people that benefit.

Well there's these good guys -- the organizations with highly targetable networks, the content distribution networks and those that provide channels for free speech, etc. Then there's the bad guys -- the criminals, terrorists and generally any organization that uses it for attach. And it's not differentiating in this section. It's just these are the people that benefit -- some good ones, some bad ones.

Marika Konings: And I think that's how it was intended as well in the other part of the report run.

Avri Doria: Oh yes. So there's no implication here that they're stealing resources to do it.

Joe St. Sauver: Okay.

Avri Doria: I must say I'm doing a fairly, you know, oral reading. Okay. Then there's line 209. Probably needs legal review or supporting evidence. Let's go to 209.

Man: In line 209?

Avri Doria: 209.

Joe St. Sauver: Again, we have line drift I think. But this is the problem of (unintelligible).

Avri Doria: Well no. We're just (unintelligible)

Man: There you go. 207 for me. Okay.

Avri Doria: 207 through 209. Is that what you're referring to?

Joe St. Sauver: Since the (est) references...

Avri Doria: Yes. Okay. So while the registrar's been prosecuted for facilitating criminal activities related to fast flux (runnings), there released one recent case where some would argue there is the appearance of complicity -- namely (ST Dullins).

And I guess that is a good point in making an accusation. And it's probably worth -- and as I'm assuming that the group is comfortable with saying that if the ICANN lawyers are comfortable with it being said. Is that a correct statement?

Joe St. Sauver: That's correct.

Avri Doria: So Marika, that kind of seems worth checking. But I have a few things to check by legal if I remember correctly. Any initial and final reports do get (record)?

Marika Konings: Yes. The final reports for sure. But I can definitely check this section.

Avri Doria: Yes.

Marika Konings: I'm just actually trying to look back at the original section to see if we provide any -- cause I remember correctly I think we do provide some links to information on the (F) case.

Avri Doria: Nonetheless, that would still be a judgment for legal counsel to say that those references were sufficient and not make him liable if somebody wanted to sue because of it.

Marika Konings: I'll check that.

Avri Doria: Yes. So I just...

Man: But I think the point is is the S domain folks were deaccredited for reasons that were not necessarily related to fast flux, at least as I read the public documents.

Joe St. Sauver: That is correct. There would be accredited because their CEO was convicted of a felony...

Avri Doria: Or else they didn't have to go...

Joe St. Sauver: ...which is a violation.

Avri Doria: ...all the way down the group. They, you know, in all things legal. They found an easier explanation.

Marika Konings: But we don't say here that that was the reason. We're just implying that there's a case where some might argue that there has been complicity between the registrar and fast flux hosting, or that's how I read it at least.

Avri Doria: Right. But one could therefore say that that's an accusation and could call -- could conceivably hold ICANN liable for making an accusation.

Marika Konings: Not (Ike) on the working group I'm sure.

Avri Doria: Then once again...

Marika Konings: No. That's okay.

Avri Doria: ...it fits all. Working group is part of ICANN you know.

Marika Konings: I will run this by the lawyer.

Avri Doria: I think that's -- I think almost anytime somebody raises the flux test just with legal counsel. That's why it's very risky not to do so.

Marika Konings: I will run this by legal counsel and see, you know, if it's not acceptable and what alternative wording we could use or would need to be done (unintelligible) unacceptable for legal counsel. Okay?

Avri Doria: Okay. Thank you.

Joe St. Sauver: I was going to say if you could just drop those two last words, and I think then probably the rest of it would be fine. It's just the specific accusation (unintelligible).

Avri Doria: Right. Now I have a question. I mean and this is -- do we need the named reference? Does it add anything other than liability?

Marika Konings: Again, then we would need to go back as well...

Avri Doria: Right.

Marika Konings: ...to the relevant section on Page 34 where we do talk about F domains and the (flower) and the (color) takedown. I'm just going to quickly read. If we say anything similar there or whether this is just a statement of what happened, what actually (unintelligible).

Avri Doria: (Unintelligible) Yes. But it's (very) remove more than two words. You'd have to go and do all kinds of stuff.

Marika Konings: Well because the year as well there's another sentence like fumbling at first as an executive summary, it has a lot of activities surrounding their involvement with a disproportionately large number of fraudulent domain names, including fast flux domain has been widely reported in the press, along with the conviction of the president for money laundering and credit card fraud. So we do have a reference there at least to an article that -- and we need to look at the middle I'm kind of saying.

Avri Doria: But there's also a difference between the weight of it being in the executive summary and listed the way it is now. And now if you don't move anything in the executive summary if you take it out...

Marika Konings: Okay.

Avri Doria: ...you can leave it in the other place. I was still concerned with counsel. But I think that might be a safer route because in this place it's, you know, you're then going with all your evidence. So I would recommend if no one objects dropping the first reference but leaving the rest of it alone.

Anyone have a problem with that? But I would also confirm with legal counsel just to that even the 961 through 72 doesn't need any rewording. That okay? Anyone object? Okay. Did people receive the rewording that Joe sent out yet? Has that even pierced through the list? I don't think I've gotten it.

Joe St. Sauver: I shipped it out. Our mail is probably slow today.

Marika Konings: Well we had some issues before on receiving e-mails that were sent to a mailing list. So it might take a bit of time.

Avri Doria: Okay, in which case I'll get going on it. I just wanted to (unintelligible). Okay. Then we got -- we had Martin. Okay. I've got Joe's. Let me stop and get Joe's. Hurry because I'd like to deal with this now if we could. Wording for line 109 -- I got it. But it's still loading. I don't know what's going on. I'll come back to it. And then I say that then something happens.

Okay. I got it. Rapid and repeated selection of systems from a pool of botted hosts with those systems being used for the purpose of hosting malicious content, or used as name servers and for other purposes of all the DNS entries with low TTL. Those seem very can't make a mistake meaning about -- anyone object to that wording that Joe sent around? No? Good. And you either have it already, Marika, or it's there.

Marika Konings: I have it.

Avri Doria: You have it? Okay. Good. Okay. Then the next set of issues we had were from Martin, which also goes into the one thing we discussed from the last call was reviewing the document for any refinements, in light of the new metrics.

And after reviewing the document again, the only place that seems like since approach taken by walking group. And I suggested we include an additional paragraph in there, and then give basically the line.

The group decided it would be useful to reference information from organizations to the past president for main analysis work. The material is attached to this report as an annex. A good line -- where would you -- what line would you recommend putting this in?

Martin Hall: Give me one second. You do it after the second or third paragraph (unintelligible). Trying to get to the right page.

Marika Konings: It's Page 19...

Martin Hall: Yes.

Marika Konings: ...if it helps.

Martin Hall: Make it the second paragraph I think would be my recommendation.

Avri Doria: I was going to put it after 515. And it's the one line paragraph. That's (unintelligible). I would almost recommend the third.

Martin Hall: I'm fine with that, too, I think.

Avri Doria: Because (unintelligible). But it really doesn't matter. Does anyone want another? I think -- does anyone object to the fact it's going in? No objection at this time. So again unless you're aware -- Marika, what are you thinking where it makes a lot of sense?

Marika Konings: Sorry?

Avri Doria: Where do you think it makes most (unintelligible) -- after the first paragraph or after the second?

Marika Konings: I would say after the first paragraph I think.

Avri Doria: Okay then.

Marika Konings: It's talking about the process while the second paragraph already talks about the number e-mails and things like that.

Avri Doria: Okay.

Marika Konings: And either you don't want to go into...

Avri Doria: Okay. We'll put it in and see how it looks and if it feels right. Okay. So in terms of the -- before we're talking about the annex. In terms of the first part of the argument -- I mean the discussion, we've got two things pending. We've got a adding numbers to the charter questions in the summary to make it clearer for the headings to touch -- to make it clearer what's being done there.

And we've got checking with legal on the issue of that one specific reference. Other than that, are there any other issues pending in the main part of the document? Other than those two which we'll get a quick view of and can do like a 48 hour last call on over the e-mail list, we're fine with going forward?

Any objection to that? Great. Okay. Moving to the next -- So then what other changes that we need to (unintelligible). Here we are. The next one first -- and which annex specifically do we want to look at now, the metrics one or any of the others to that effect? Now I'll look at (unintelligible) statements which haven't changed in forever.

Marika Konings: Nothing has changed there. The only change has been made to the annex is the adding of the data annex that Martin provided.

Avri Doria: Right. Yes.

Marika Konings: And one note maybe to make as well on the supporting or additional statements. There is currently one -- the individual statement. There's one from Mike O' Connor. Previously we had received two other statements -- one from Eric Brunner-Williams and one from Christian Curtis.

I've written to both of them with one of the latest drafts of the report asking them whether still wanted to attach their statements to the document, as a lot has changed between when they submitted their statements and then the latest version.

I only got a response from Eric Brunner-Williams. And he was going to review the document and get back to us which is already I think more than a month ago. And I didn't hear anything from Christian Curtis. So for now I didn't include them.

Avri Doria: I would actually include them.

Marika Konings: But some of them are relating to certain issues that are no longer relevant or that have been addressed. So that's why I wanted to...

Avri Doria: Right.

Marika Konings: ...clarify with them...

Avri Doria: You would include them with notes saying they were submitted early in the process before, you know, multiple changes were made to the document and have been left in for completeness sake.

Marika Konings: Yes. I'll ping them one more time as well to make sure I'm going to be given a chance as well to respond themselves. And if not, I'll include them back in.

Avri Doria: Right. I just -- I'm very unsure about basically almost devaluating the whole document because we excluded somebody's personal comments, other than we said we would include them.

I have no -- I think though it's quite reasonable to attach a note above that says, "You know, these personal statements were submitted early in the process and, you know, do not reflect comments based on the current document but on the earlier version of the document." And leave it at that.

I mean that's the thing for Mike's, too. They're all the statements that we have are statements from mid-term in the process. And so a statement that just identifies them is I think would be fine. And then it's a complete history. Anybody object to following that -- making a pattern?

And then yes, certainly check with them again. And if they withdraw it, then they withdraw it. But if they don't you not going to -- especially having asked if we can remove it. And then remove it with them having said so and just open us up to, you know, as far as the (unintelligible). It's not worth dealing with.

Marika Konings: Okay.

Avri Doria: Oh yes. Okay. And I can help you with the wording of that caveat if you'd like. But I'm sure you can do it without my help.

Marika Konings: Yes. I think you already provided me basically...

Avri Doria: Okay.

Marika Konings: ...the wording. Just not (unintelligible). But that's fine.

Avri Doria: Okay. Thank you. They'll say that is in my handwriting. Any other issues on it? Any issues on the metrics pages? We've talked about it before. I think it's quite strong. I just want to make sure that there are no last comments. Okay. Any other issues before we sort of call this waiting for last call?

Marika Konings: Maybe one comment from me or...

Avri Doria: Yes.

Marika Konings: ...I'm happy as well to add to the final version as a post text for the public comment period, that normally goes together with an announcement and like a little box it provides some information on what the working group...

Avri Doria: Yes. I can do that.

Marika Konings: ...is looking for.

Avri Doria: You mean just the cover letter as it were?

Marika Konings: Sorry?

Avri Doria: What do you mean the...

Marika Konings: Yes. The announcement that goes with...

Avri Doria: Right. Yes.

Marika Konings: ...the public -- the launch of the public comment period. So I'm happy to draft the text for that so the group can review that...

Avri Doria: Okay. Great.

Marika Konings: ...and make sure...

Avri Doria: That'd be great. And I'll remember -- we can do that on the list as well. Is a 48 hour last call good enough? Or do we need a longer one? How are people in terms of that? That's basically to have a last look at things and say yea or nay.

And then the way I've done them in the past and when it's just okay is I call the 48 hour. And then if there is anything that needs to be changed we discuss it. And from each of the -- and it's basically a rolling 48 hours. You know, there's a -- well I'll propose a solution. Now okay. Is this solution acceptable for everyone? And then we roll 48 hours.

Marika Konings: And I guess the 48 hours starts after the posting of the final version.

Avri Doria: Exactly.

Marika Konings: Okay.

Avri Doria: Wait. No, not now obviously.

Marika Konings: Okay.

Avri Doria: (Unintelligible) Oh yes, after it goes out ask the question when you said they (unintelligible). Please let me know within 48 hours if they'll soon decline. If someone has an objection, then it gets fixed. And then the 48 hours rolls on until we basically had 48 hours of nobody saying there's an issue. And hopefully we don't have to have another meeting on it at this point.

But I'd really like to get it out as soon as we could now that it's all there and ready to be talked about in Mexico City, and especially when the council back in and figure out where we go from here. Now is that okay procedure? Does anyone object? Mike, are you okay with that?

Mike Rodenbaugh: I'm good with it. Thanks.

Avri Doria: I had to call you out to remember that you're here. It's hard to mention the council on this one. Then we'll go for...

Mike Rodenbaugh: Have to just make sure that if we get the report to the council as soon as we can. And ideally we can discuss it in our February 16 meeting.

Avri Doria: Yes. Well we could certainly discuss there the process that the council is going to take. We obviously don't want to get into substance probably until after the comment period. But anyhow we should talk about that in council certainly.

Mike Rodenbaugh: You're right. Yes.

Avri Doria: Okay. Any other issues? Okay. Then at the moment we'll do that. And then I think this group will basically go into sort of a holding state until we find out on the council level where we continue. Does that reasonable to -- I mean certainly people can continue using this mailing list to this group of people to discuss issues. It is interesting.

But we won't necessarily have any meetings or goals. And as I say if we come back to the working group with more work, it's my full intention that there'll be a new and different chair at that point, because I think I should not play chair of council and chair of (unintelligible) at the same time. So I'm glad I did this. And I'm glad I worked with your all on it.

Man: Been a real pleasure.

Avri Doria: Okay.

Man: Yes. Thank you.

Avri Doria: Thank you all. And I'll talk to you all soon.

Man: Have a good weekend.

Avri Doria: Okay.

Man: Great. Thank you.

Avri Doria: Have a good weekend. Bye-bye.

Man: Thank you.

Marika Konings: Bye.

Man: Bye-bye now.

END