Fast Flux PDP WG Teleconference
TRANSCRIPTION
Wednesday 8 April 2009 14:30 UTC

Note: The following is the output of transcribing from an audio recording of the Fast Flux PDP WG teleconference on Wednesday 8 April 2009, at 14:30 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-20090408.mp3
On page:
http://gnso.icann.org/calendar/#april

Present for the teleconference:
James Bladel - GodaddyRRc - Working Group chair
Greg Aaron - Afilias Ry c.
Paul Diaz - Networksolutions RRc
Ihab Shraim - Markmonitor.com
Avri Doria - GNSO Council chair, interim working group chair, passed chair to James Bladel.

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

Staff:
Marika Konings
Glen de Saint Gery

Dave Piscitello Good morning.

(Avri Doria): Hi, (Dave).

Coordinator: ...has now joined.

Dave Piscitello We are now recording.

(Avri Doria): Okay, thank you. Glen could you start out by reading the list of who is on the call?

Glen Desaintgery: Yes, certainly (Avri). On the call we have (Joseph St. Sauver), (Avri Doria), (Martin Hall), (James Bladel), Paul Diaz, (Randall Vaughn), (Rod Rasmussen), (Dave Piscitello), and (Greg Aaron). And from staff supporting the call we have (Marika Konings) and myself, Glen Desaintgery.

Thank you (Avri).

(Avery Doria): Okay, thank you. Okay, I want to start this meeting on the subject of the chair of this little group. We've had one volunteer, (James Bladel), and I am extremely grateful to have one volunteer for taking over the role as the working group chair to finish up this last bit of the process.

So I wanted to do a couple of things.

One, I wanted to make sure that there were no other volunteers vying for this role who just hadn't mentioned anything. Two, I wanted to mention the process - what would basically - if this group or once this group agrees to having someone new as a chair, that person could start as chair.

It would need to be confirmed at the next council meeting, but that would be - you know it has been mostly just a (vanity) check and it's not a - you know a strong a strong confirmation process. And I don't expect there to be any issue.

So first, I want to ask is there anyone else that has been dying to volunteer and just hasn't gotten around to it yet?

No, okay. Is there any objection in the group to (James) taking this role?

I'm hearing no objection. I'll take it that this group has decided that it would like to have (James) as its chair. Is there any objection to my turning over the chair of the rest of this meeting to (James) at this point? I'm hearing nothing. I will assume there is no objection.

As the departing interim chair, I thank you all for the help, cooperation, and everything in letting me do this, and (James) have a ball.

Man: I want to jump in and just say thank you very much, (Avri). It has really been a pleasure to work with you.

(Avery Doria): Thank you.

Man: Thank you, (Avri).

Man: Thank you.

(James Bladel): (Thank you everyone).

As (Avri) mentioned, we are very close to the conclusion of this process. We're probably in the last phase where public comments from the latest round and we need to design an approach to get those analyzed, categorized, and incorporated into our final report.

Does that agree with everyone's perceptions of the group are as we attempt to reboot this process?

Man: Yes.

Man: Yep.

(James Bladel): Okay, great. And you know as - I probably should point out that I'm kind of winging this. I'm new to chairing the working group, so I'm going to be relying on some of my friends and colleagues here to let me know when I step over a landmine, okay.

Man: Sure.

(James Bladel): (It doesn't always happen) this morning. Okay, well if you can, (Marika) sent out some materials earlier in the week, including a PDF, which attempted to categorize the report - I'm sorry, the comments into some basic categories. Does everyone have that document or can get to it fairly quickly?

Man: Yes.

(James Bladel): Okay, great. I'll just give everyone a moment there. So I'd like to spend the remainder of this call taking a look at maybe not the meat and potatoes of each individual issue, but just taking a look at the categories and ensuring that we agree that these categories are distinct, and their definitions are defensible, and that they maybe should or should not be combined or merged or broken out into separate categories if they become too cumbersome.

Any thoughts on that? Okay, hearing none, I'm just going to proceed then with taking a look at some of the categories that (Marika) has in her report there. (Marika), are you still available?

(Marika Konings): Yeah, I'm here.

(James Bladel): Okay, great. It looks like we have a total of - excuse me here. I printed this out so it would be a little easier. It looks like we have a total of nine categories. Is that correct?

(Marika Konings): That's correct.

(James Bladel): With Item 9 being the largest of those. So we can take a look here. It looks like the first category is legitimate versus illegitimate uses of (Fast Flux), and there's - it looks like nine possible comments that fit into that category. The one that was a little new that we were discussing was that the Category 2 is in a class by itself as the impact of (Fast Flux) on the digital (divide).

A few comments. Pardon me.

(Joseph St. Sauver): I was just going to jump in and say I really found that to be one of the most innovative and constructive comments that we received in terms of just bringing up an entirely new area that I certainly hadn't considered at all.

Man: (Joe) can you explain that a little bit, because I wasn't sure exactly what the core of the comments really meant.

(Joseph St. Sauver): Well I think what he was trying to get at is the fact that you know (Fast Flux) really adds to a lot of the network burden that some of the folks in the third world might actually experience.

I mean if you know the DNS system works the way you would hope it would work, everything goes ahead and caches pretty well and basically, it doesn't have a lot of churn. (Fast Flux) really introduces a lot more churn and implicitly sort of provides a burden on the network links as a result. A lot of these are very thinly connected.

Man: Do we know whether it's significant or not?

(Joseph St. Sauver): I'm not sure there's been a study of that to tell you the truth.

Man: Okay, but I mean it very well may be the case, but I just - I have no idea whether there actually is an impact or not.

(Ihab Shraim): This is ((Ihab) Shraim). I've seen an impact on say certain networks only when (DDoS) has been imposed through (Fast Flux) or a massive marketing campaign by which (Fast Flux) has been used by which you know probably a major email campaign has been - gone out. And that definitely will impact certain networks, specifically the networks that are transmitting the data if it is a marketing campaign.

As for (DDoS), you know the recipient network or networks will be impacted drastically.

(Joseph St. Sauver): So you've seen it in conjunction with an email campaign.

(Ihab Shraim): Yeah and the - as you know, they can (rent) these sites, but most importantly, somebody would want to distribute - if you notice, the amount of spam has increased recently due to the fact that you know (every brother) would like to just send something. But yes, the email

campaigns do happen illegally and these networks are being used, and they do take a portion of the bandwidth allocated for each network.

(Joseph St. Sauver): Now you're talking - now spam is sent from BotNets, but how is the spam related to (Fast Flux)?

(Ihab Shraim): I don't want to say it's mainly spam. I want to say it's utilizing the (Fast Flux) networks themselves to distribute or to impose something on the receiving party. (Fast Flux) of course mainly - and in my opinion when it affects the network, it's (like) a (DDoS) attack.

(Joseph St. Sauver): Okay, we have to be careful to distinguish BotNet activity from (Fast Flux) activity. They are two related but separate things.

Now the Web site advertising a spam campaign could be hosted on a (Fast Flux) network, but the spam is not being sent from (Fast Flux) (domains).

(Ihab Shraim): Fully understood. That is a correct statement.

(Joseph St. Sauver): Yeah and then (DDoS) would either be inadvertent because of the level of traffic or it could just be an explicit (DDoS) attack. But that doesn't use (Fast Flux); that just uses a BotNet to send traffic.

(Ihab Shraim): Actually, you can use a (Fast Flux) network with (DDoS) attacks. Now I'm not saying you know of course (BotNets) where you begin everything - your spam campaign or the initial action. But you can - there are regulated (DDoS) attacks that are being done now.

The initial (DDoS) attach that (we know it) were a site can be just hit with - to fill the bandwidth pipes have moved to another style of (DDoS) attack by which they hit you at certain peek times without (filling) the entire bandwidth and then it disappears. And you can only do that via manipulating (Fast Flux) networks.

(Joseph St. Sauver): Well we've been mainly talking about (Fast Flux) as a way of hosting some content in the way of avoiding detection. So I'm still - I still don't understand how the spam is related to (Fast Flux) other than a site advertised in a spam campaign.

(Ihab Shraim): No, well said. I think they can be intermixed a little bit, but (bots) are the sender of any spam campaign vis-à-vis the initial discussion begun with how do you impact networks, and normal networks are impacted as I started by comments with (DDoS) attacks.

(Joseph St. Sauver): Okay.

(Greg Aaron): All right, I don't - this is (Greg). I don't want to belabor the point.

(Martin Hall): (Greg).

(Greg Aaron): Yeah.

(Martin Hall): Can I chime in? This is (Martin). My understanding of reading the comments - and I'm listening to (Ihab) and I there may be something worth noting there. But my understanding was this had to do with the frequency of zone file updates over these thin links that (Joe) is talking about. (Joe), correct me if I'm wrong in terms of my understanding, but I thought that was the issue that was being raised.

(Joseph St. Sauver): It's been a while since I looked at (Woody)'s comments. I may have gotten it wrong, but my impression was just that it was a general level of traffic that they were going to - EDP traffic. And (Martin) are you talking about zone file updates at the TLD level or below the TLD level?

(Martin Hall): Well starting at - well potentially both depending on the type of flux that we're talking about.

(Rod Rasmussen): This is (Rod). I had the same impression as well. He is really talking - it has nothing to do with malicious use necessarily. It was more about the fact that if you are using (Fast Flux) networks whether it's (ACAME) or the Russian Business Network. Whoever it is, it's acting - just in general, the level of DNS updates (unintelligible).

(Joseph St. Sauver): That's my understanding. I concur.

(Martin Hall): If this was - I just wanted to just go back to (Joe)'s point. This was the single most interesting comment to me out of everything that we got, and I'm not sure that we had anything really in the report that addressed you know the impact on bandwidth and this you know so-called digital divide. And it might be worth some lines of addition to the report to talk about bandwidth implications and we can potentially separate that into at least two areas.

Number one, there is the - you know the frequency of zone file updates and the impact on bandwidth. And listening to (Ihab), it may well be worth noting that you know where there are (BotNets) that compromise

computers that sit behind these thin links, then there may be bandwidth implications from that as well.

(Avri Doria): This is (Avri). Can I point out a secondary effect that I think may be relevant? It's not only bandwidth within the digital divide, and that's one of the areas I spent a lot of time in. But within the digital divides because of the payment methods they have, they are actually paying for all traffic that is both sent to them and that they send.

So there's also - if the bandwidth usage is increased by this, there's also a real financial impact. So they both have narrow pipes and they pay for everything that goes down them in both directions.

Dave Piscitello This is (Dave). I think we also have to pay attention to the fact that this is not simply you know an infrastructure that could be exploited for Web and traditional IT traffic, but also for SMS over voice network.

And again, you know it's not only the bandwidth you know, but you know the remarkable cost that is going to impose on people and the ability to do that in a very, very large-scale manner in a very, very pernicious way to attack a particular population or culture.

(James Bladel): Excellent point. This is (James). It sounds as though that this is - this comment in particular is very thought provoking and raises a number of issues.

One of the questions I would put to the group is can we do this justice as an add on to our report, or should we possibly recommend - maybe perhaps reference this comment and then recommend a larger study on this issue as possible next steps? Any thoughts?

(Joseph St. Sauver): Such a study might be interesting. I'll also say that it will take a lot of time and it is a fairly - it seems like a fairly complex project.

(James Bladel): Okay, do we want to then try to at least give it a cursory treatment within our existing report?

Man: Yes.

Man: Yeah, I agree.

(James Bladel): Okay and we can then separate that out from the other comments. Do you believe that it merits its own - you know from an organizational perspective, I see a category of one on Number 2 and on Number 8. And you know I'd love to find a way to merge Number 8 into one of the existing categories or find relevant items elsewhere that can be used to further substantiate that category.

But it sounds as though Item Number 2 in Mr. (Woodcock)'s comment would be that we should flush that out a little bit more and touch on that in our report.

Thoughts? Agreements? Disagreements?

(Avri Doria): This is (Avri). It seems to me that doing you know a little bit of expansion on it and putting it in there with perhaps a pointer that it needs more investigation. So basically, following sort of both approaches that you have seems reasonable.

Dave Piscitello Don't we already say that law enforcement would benefit from the cessation of (Fast Flux) attack networks?

(James Bladel): I'm sorry. Could you repeat that? Was that (Dave)?

Dave Piscitello Yeah, I mean I - if we did not say that (law enforcement) would benefit from the cessation of (Fast Flux) attacks that would be - I thought we had enumerated that as one of the groups of people who would benefit. So it seems like a relatively small addition to a long list of people that you know would benefit from cessation of (Fast Flux) attack networks.

(James Bladel): So you're jumping to Category Number 8, Mr. (Gary Warner)'s comments regarding law enforcement. It seems to be very closely related to his comment Number 7 about if criminals benefit, then clearly law enforcement would benefit from its cessation.

Dave Piscitello Right.

(James Bladel): Any thoughts on merging 8(A) and 7(B) from (Marika)'s list into sort of a compound comment? I mean obviously we can't merge the language of Mr. (Warner)'s comments, but at least for categorization purposes.

Dave Piscitello It's all in the same section. I think they are both relevant and it's more or less just trying to complete the list.

(James Bladel): Okay, good point (Dave). (Marika), does that make sense?

(Marika Konings): Yeah, I think if it was separated here because they were two different questions that were - part of two different questions that were

asked as a charter question. So I think that's why I broke them out here.

(James Bladel): Okay.

(Marika Konings): But no problem in merging them.

(James Bladel): Were there no other responses that discuss benefits - folks or parties who would benefit from the cessation of (Fast Flux)? Is this the only comment on that question?

(Avri Doria): This is (Avri). I don't see any problem with leaving it as a separate category in the comments. I think once you get to the fourth column of where it got fixed or where it got dealt with, then you'll find it's the same (page) as the stuff from 7.

But leaving its visibility is one of those good things for afterwards when you sort of attach this table perhaps to the back of the document that shows you know these were the comments and this is how they were dealt with. Keeping it separate seems to have that visibility advantage.

(James Bladel): Good point. Any thoughts on (Avri)'s suggestion? Okay, well let's proceed that way than leaping in - separate but to gain some visibility and then address where appropriate when we're discussing our comments.

Were there any other categories that were listed that folks thought perhaps were - could be broken out into multiple categories? And right now, I'm just kind of looking at item or Group Number 9, which has a -

I'm trying to count the letters here, but it looks like about 20 different items. Is that correct, (Marika)?

(Marika Konings): Yeah, I think so.

(James Bladel): Yeah, so I just - looking at that category, I'm wondering if there are any opportunities to further subdivide that category. Let's propose for next steps and possible solutions if we could identify who would be carrying out the next steps, or if there was a sequence required, or any dependencies or interrelation between these proposed steps. That might be one opportunity to further provide some resolution on this category.

(Rod Rasmussen): This is (Rod). I'd say there's a natural divide here because of concrete actions and specific details versus more study of X because you have lots of different comments about more studies.

(James Bladel): Okay, that's a good point (Rod). So some of these are actionable and some of them are requesting additional information.

(Rod Rasmussen): Yeah.

Man: Some of these are also specific directives to system administrators or operators either at the end point or at the edge or in the core. So we might be able to look at that.

For example, securing applications with technology and filtering and white-listing are all things that are kind of standard litany for how we apply countermeasures in other you know attack sectors. And so we

might - you know we could probably go through this list and (approve those).

(James Bladel): Okay.

Man: There also seems to be a significant number of registration oriented (unintelligible) that might be (fed) into one of the other groups that's looking at registration of (use).

(James Bladel): Okay, so that was - you are suggesting that some of these might feed into other activities or working groups. Did I understand that correctly?

Man: Yeah, I mean I know for a fact that for example 9(N) is something that (FFACT) is looking at now and will probably publish something by (Sydney). So asking (FFACT) to you know take a look at this would you know be kind of a self-fulfilling prophecy since we're already doing it.

I think that you know adopting the accelerated domain suspensions and several other APWG-oriented statements here kind of suggest that one recommendation is to explore further - for the GNSO to explore further some of the valuable contributions that the APWG has made in this area or in the general area of you know - of mitigating of (use). That's already underway.

(James Bladel): Okay, so it sounds like we have a couple of ideas and maybe we can adopt them both to further subdivide Category 9 into those comments that are direct actions or those comments that are requesting additional information. And then one or both of those categories can be

further subdivided into who would be the targeted audience or recipient or let's call it owner of the action item would be.

Man: Yeah.

(James Bladel): Should we break this into three categories or four?

Man: Can we go ahead and go over why we're breaking them up? Is it just to go ahead and try to highlight the underlying themes or...?

(James Bladel): I'm sorry. I didn't catch that last bit there - while we're breaking them up.

Man: I was just asking why we're going ahead and working on trying to subdivide them further. If anything, I would be kind of inclined maybe to try and pull them together into fewer clumps, but...

(James Bladel): Okay, well I think that if we are looking at what actions specific groups can take, then we can definitely fold those items in with Number 4. There seems to be some overlap for Category 4 because now we're talking specifically about what actions registrars and registries can undertake. So that kind of builds on what (Dave)'s comment was about when we were talking about systems administrators or those who are in control of the (end notes) - what role of ICANN.

So it seems like there's perhaps some correlation with Category 4 and Category 6 with a subset of Category 9.

Any thoughts on that approach?

Man: Are you basically just trying to go ahead and change it from sort of a topical focus to an actor focus in terms of like who is going to have to do things with these, or...?

(James Bladel): I'm just pointing out that if we break up Category 9 based on who the next steps are directed towards, then that sort of implies that some elements in Category 4 could also fit into that group.

Man: Okay.

(Marika Konings): This is (Marika). I thought (Avri)'s suggestion made sense in saying doesn't it make sense to see where these would fit into the report and then you will see indeed which ones actually belong together and (form a theme) instead of maybe breaking them up here.

(James Bladel): Okay.

(Marika Konings): Because then we're just subdividing the table and actually I don't think we're getting them to - it might take longer than getting them discussing where they belong in the report if at any (pace) or whether they are already addressed or not. That's (sort of the best thing for that).

(James Bladel): That's a good approach as well. In that case then, we would probably want to take a look at the categories in terms of the sections that we have in the report and the different charter questions. Is that correct (Marika) if I'm understanding you?

(Marika Konings): Yeah, I think that's - you know what I'm trying to say what (Avri) said that you know you would come to see which points belong

together if you discuss why they would be incorporated into the report or why they have already been discussed. So you can see them in you know the fifth column once you have filled that in or discussed that - which comments are actually you know part of the same group or belong in the same spot. I think - (Avri) did I interpret you correctly?

(Avri Doria): Yeah, no that's pretty much - I mean one possible way would be to sort of accept the division because it's really just a way to make things visible and start marching through them having discussions of, "Look at the first (one's view) of the working group. Oh, well no that's already covered," or, "Oh, good point. Needs amplification."

Or how to scope, (end scope) and make all of those decisions for your fourth column. And then whenever the decision - (end view) of the working group was, "Hey, we need to add something to the final report," then you go to the final column and you say, "Okay, where does this go?"

And then you'll see after you've done a first march through as it were that, "Oh, okay these things were in Section 7, these were in 6, these were in 4," and then you've got a second natural grouping of where the work and the word-smithing needs to be done.

(James Bladel): Okay, so what does that group think of that approach? I think that's a sound way to proceed. Then the question would become we would just essentially dive into the first category and try to identify where that - where those items fit. And then a possible work plan for this - the remainder of this meeting. It looks like we have about 25 minutes remaining. Is that correct, (Marika)? We would just...

(Marika Konings): Correct.

(James Bladel): Yeah, we would just continue with Section 1. It seems like we had a really good conversation on Section 2. I'm certainly not opposed to taking these out of sequence if we have the right parties and expertise on the line to tackle something that's in a category of its own first.

Okay, well let's take a look then first at the comments that are in Question 1. Any objections? Okay.

Looking at Question 1(A), there was a comment from - it looks like (R. Atkinson). The distinction between legitimate - all of these are going to discuss legitimate versus illegitimate uses of (Fast Flux), and I think that we've covered this fairly extensively within our report. Is that correct, (Marika)?

(Marika Konings): I think so.

(Avri Doria): What would (Ren) mean by a clearer distinction?

(James Bladel): Good question. Possibly a viable value for TTL so that we understand what low and what high means - what an obvious versus non-obvious reason would be.

Dave Piscitello (Ren Atkinson)'s comment was fairly long and yeah touched on a number of different issues. I think one of the things that we could do is - someone could just go through it. I'd be happy to do that.

I know for example that one of the issues that he wants to raise that hadn't been raised you know was that one of the legitimate

applications of (Fast Flux) that we did not cove was you know the way it is employed in mobile networks.

(Ren) if you don't know is one of the principle developers of mobile IP - you know (RFC)s. So you know referring to his expertise there is probably you know quite valuable for us. But if you want, I will go - I will be happy to take - you know take his comment and sort of summarize what we might want to include in the report from it.

(James Bladel): That would be fantastic (Dave).

Dave Piscitello And I don't know (Ren) fairly - I mean I haven't talked to him in probably ten years, but I know him well enough where I can ask him for specific - you know specific feedback or clarification. So you know I'm happy to do that.

(James Bladel): Okay and just as we go through this, I imagine that may come up with some of the other commenter. (Marika) and (Avri) is there any process or protocol that we should be aware of when reaching out to folks who submitted public comments or further clarification?

(Avri Doria): I don't think so. I think you know any time someone wants to contact. Obviously if there is someone on the group that knows them personally or well, that's the easiest path to take. But no, there's no formal. I mean you know, "I'm working in the working group. I've read your comment. It's interesting, but can you tell me more," kind of note makes sense.

And yeah with (Ren), I mean I also know him. But it's good that you know (Dave) would contact him and ask for clarification. And I'm sure he would be more than willing especially when you get to one of his

later comments that's you know - and hey once this is here, passing this over to some of the (IATF) groups was really you know a good thought.

(James Bladel): Okay, thanks.

(Avri Doria): Is he still on the (IAB)? I forget.

(James Bladel): I'm sorry.

(Avri Doria): No, I was just wondering to myself if (Ren) was still on the (IAB) or whether he wasn't anymore.

Dave Piscitello I don't think he's on the (IAB) any longer, but I do believe he continues to participate in the (IETF).

(Avri Doria): Yeah.

(James Bladel): Okay, so then (Dave) you are going to take a look at his comments in greater detail and possibly reach out to him for clarification or questions.

Dave Piscitello Yeah, I mean if there's something that I sent you - something I don't understand at least well enough for us to summarize. I mean obviously we're not going to write a litany about mobile IP, but you know if there's something in his comment I will be happy to - you know happy to reach out to him. So I'll try to do that by our next teleconference.

(James Bladel): Okay and is there a possibility that his comment is driven - that there's some specific aspect of mobile networks that we overlooked.

Dave Piscitello I think that I'd have to go back and read the whole comment, (James). You know I just recall that when I read it, I said, "Yeah, we forget mobile IP, didn't we?" So I just need to you know re-immerse myself in it. I mean it was fairly lengthy. It was several pages of an email.

(James Bladel): Okay.

Dave Piscitello So but I'll tease through it and pull out the issues that I think we should raise in the report and I'll post them to the mailing list.

(James Bladel): Okay, thank you. I appreciate you looking into that. So if there's no other discussion of 1(A), we can move on to 1(B). This comment submitted by (Claus) seems to have a lot of - at least reading the summary; it seems to echo a theme that's very common, which is that the individual is disputing that there is a legitimate purpose or use for (Fast Flux) at all.

Dave Piscitello Actually, this is something I was going to ask (Avri) about. You know when somebody states something that the working group has clearly - you know clearly come to a counter-conclusion, what is our obligation?

(Avri Doria): I think that in our explanation you know and the response that we publish to things basically say that you know, "We appreciate the comment, but we have these various legitimate reasons or whatever you know that could do that." That I think there's basically an obligation to say, :"We've heard the comment, we've discussed it, we've gone back and looked at any new stuff that you've mentioned that perhaps we hadn't thought of and yeah, you know we remain where we are or we've tweaked A, B, C based on what you've said."

But you know I think we have to take the comment, look at it, and make sure there's nothing new in it.

Man: In some cases, I think it's almost as if the person commenting may not have had a chance to review the entire report if you get my drift.

(Avri Doria): Yeah and sometimes you know when reading something, they may not see the emphasis is there as clearly as they might have like to. So there may be a tweak or two in the wording that you get from you know the content of what they say.

But no, I don't think you need to change the report before you get a comment. Because if you get a comment that's opposite, you just need to think it through and say, "Yeah, no we said the right stuff. We said what we meant to say and this is why."

(James Bladel): That's a good observation and good guidance there. One other possibility would be if we see a large number of comments on something that is maybe not as visible as it needs to be in the report. We can find different ways to highlight that, moving it into its own section or possibly drawing better attention to something if we see that there's a great deal of confusion or that it's just drawing a lot of comments that we weren't expecting.

(Avri Doria): The other thing that you might do - I mean since we have places in the report that say you know strong support, some support -- I'm not getting the words right at the moment -- and alternative views. You know if a comment strongly backs up an alternative view, you know we can add something that says, "And there were comments received

from the community that emphasized this view." You know so that the full content is there, but you certainly don't need to change it unless of course your mind is changed by what they say.

Yeah, if somebody comes up with a really great reason to refute something that you all you know thought of and said, "Oh, yeah right. I hadn't thought of that. Yeah, of course." And you know I don't expect that to happen a lot, but that's always - that's an open possibility.

(James Bladel): Right. Okay, so I think that there's a lot of similarity between this comment, Comment 1(B), and it can probably be addressed similarly with Comment 1(C) and 1(E). Does that make sense that a single bit of language perhaps can identify the comments - those three comments and perhaps reference them simultaneously.

Dave Piscitello I would imagine that with the exception of 1(A) and 1(G) that we could - you know a summary comment that explains that we've - you know what - reemphasize what the working group concluded is sufficient.

(James Bladel): Okay and just turning the page here and looking at H and I, and I think that those would support what you're saying, (Dave).

Dave Piscitello I mean that's - I guess the only thing I would imagine perhaps I would you know (process) to do would be to look at some more recent work in distinguishing (Fast Flux) networks from - you know legitimate uses from (Fast Flux) attack networks. I just don't know how much - you know how much bandwidth this working group has left to do that.

So we might want to say that we encourage continued study into the dynamics then that - you know and the changing attacks (surface).

(James Bladel): Okay, thoughts from the group. I think the proposal is to take a look at 1(A), 1(G), and possibly 1(I) individually and then perhaps group together the remaining items in Section 1 as being sufficiently similar that they could be addressed by a common paragraph or section.

Man: What about 1(H)? (Casey) is an awfully influential individual and usually has excellent comments and I have to admit I agree with her comment in this case too. I don't think 1(H) deserves to be kind of just lumped with the others.

(James Bladel): Okay and maybe there's something that I'm not getting from the summary that's in the larger comment. Is that...?

Dave Piscitello I think the whitelisting - if we haven't - I can't remember whether we expressly called out whitelisting as you know a way to adjust false positives. Is that certainly something we could put in? I actually think that the statement that she makes up to the point where - you know to the first comment where, "There are so many measurable differences. It should not be difficult to separate them," is a very, very legitimate response for us to include in our responses to the other people.

(Avri Doria): Yeah, especially remembering (Casey)'s background as probably the most proficient person in the Internet at measuring what's going on at (some levels). You know it may be interesting to know what she actually (means there). She is a measurer more than (most).

(James Bladel): So is this an opportunity for us to reach out to (Casey)? I mean (Avri) did I misunderstand that there...

(Avri Doria): Well I'd need to go read her comment completely, which I haven't done. But I - you know and perhaps that's something that you know I could take a look at. I haven't seen her in a couple years, but talk to her every once in a while. But...

(Greg Aaron): This is (Greg). I think what she is saying is there are enough indicators that you can reliably figure out whether it's a bad site or not. And what we did in the report was we said - we mentioned a lot of those indicators. We mentioned the need to avoid false positives, which is something she mentions.

I mean what we're - what I think she is saying is it's fairly easy to figure out which sites are bad or not. But she also says we need some additional mechanisms and policies to make sure you don't finger somebody accidentally. And I think we said that in the report.

Dave Piscitello I know that (Casey) had seen some of the other comments before she made hers. And you know part of this was a reaction that she had to, you know, some of the other comments. And you know - I mean (Casey) is not - you know doesn't (suffer silliness) too readily. So I think that she was quite exasperated that some people would say you know some of the things that were said and they are sort of more terse and frankly less informed comments than hers.

(Avri Doria): And another thing that (Dave) points to is perhaps some - you know something that can happen in the actions you know or things that can be investigated later in terms of ways to do this. The whitelisting may be something if it's not already in the report. It can be included in possible avenues that people can look at.

Man: (What would folks think of as) maybe a table separating or highlighting some of the differences between legitimate and illegitimate uses of (Fast Flux)? It tends to respond to that comment.

(Avri Doria): Well is it the uses or is the things that are measurable differences between them?

Man: The measurable (diffs).

Dave Piscitello That might be interesting to see you know so we can - I mean I think it would be a useful experiment or you know experiment, but useful exercise for us to - you know to perform. And if it looks like it (would add value), it does in fact you know address some of the questions or you know some of the comments that we should you know make - (call) more of a distinction between the two. So we would satisfy (Alan Murphy)'s comment in 1(I) by adding a table that calls more attention to, you know, to the differences.

(James Bladel): I'm thinking that we did - and it's been a while since I - I'm trusting my memory here. But did we at one point attempt to inventory all of the (unintelligible)? Familiar to anyone else?

Dave Piscitello I lost almost all of your comments (James). I'm sorry. My connection is not all that great.

(James Bladel): Okay, it just sounds very familiar that if we were to try to - we're talking about not necessarily these legitimate versus illegitimate uses of (Fast Flux); we're speaking specifically on our metrics that we would use to detect (Fast Flux). Am I understanding this approach correctly or...?

Dave Piscitello Yeah.

(James Bladel): Okay, so these are essentially the red flags.

Dave Piscitello I would think so, but that's the way I interpreted it.

(James Bladel): Okay, (I think I heard (Avri).

Man: I was just going to say it looks like there is actually some emphasis on use in the two comments -- the (H) and the (I) -- rather than just you know abstract issues. So it really does touch use (Avri) as you were mentioning.

(James Bladel): And as it mentions use, then that starts to seem very familiar to me that we - that's familiar territory from our report where we were illustrating all of the different uses - potential legitimate uses. Is that sounding familiar to me or to anyone else or...?

(Avri Doria): Well actually - I mean as I said, I need to read the comment because it's talking about more behaviors. So the second comment (down) - (Murphy is the one) who is talking about use. But perhaps the answer to the (I) and one of the things that I'm noticing while I'm sitting here talking is even though I've read the thing many times, it's been a month since our last - more than that since I last read it. It has left a lot of holes in my memory and I'm going to need to read it again before I talk too much more.

But (Casey) seems to be talking about behaviors, which are things that can be observed. Your red flag perhaps or a white flag or green flag or whatever they'd be called that are behaviors that are actual things that

can be seen or measured on the network where as the (Murphy) comment seems to be talking about you know additional information on how to separate legitimate use.

Now the answer to that may be you can separate them by using these measurable behaviors you know to some extent, et cetera. But behaviors and uses are slightly different.

Man: By the way, should I be - actually be a part of 1 instead a part of 5 - that's to (Rush)'s comment.

(James Bladel): Is (Rush)'s comment legitimate use of (Fast Flux) that do not use (a hijack bot). So essentially, we're going back to the idea that it's - that one of the key distinguishing points of legitimate versus illegitimate is whether or not it's on a compromised (system).

Man: Correct. And since 1 is legitimate versus illegitimate, it just seems like 5 really almost cries to move up to 1.

(James Bladel): That's an excellent point. I would be in favor of moving of moving it.

Man: Haven't we made that pretty explicit in the report?

Dave Piscitello I think one of the things that we tried to do in the report and one of the things that I - is that I know I've tried to evangelize that - I talked about what we learned through the report is that you know no one indicator suffices here. And that you know there really is you know a need for considerable analysis you know to essentially draw the conclusion that the network is an attack network or it's - you know or the purpose is for some productive legitimate use.

And I really hesitate to try to - you know try to answer each and every one of these by saying, "Yes, that's correct. No - you know yes, that's sufficient." Because we know that its (evolved) at least twice already and the (variants) continue to appear.

And so trying to say, "Okay, well we're not going to you know consider TTLs for this reason or we're not going to consider the compromised - or that a bot executable on a compromised machine is - you know is one of the markers," is pushing us back to a point where we floundered for a very, very long time.

So I just want to be - I just want to caution us not to - you know not to overload some of the - you know some of the obligation to respond with - you know with making this too complicated.

There are some people who are going to look at the report and maybe seek in the (final) report for some absolute cookie cutter way to be able to identify - you know identify (Fast Flux) attack networks. And we know that that doesn't exist yet, and it may never exist. So I just want to caution us not to get tempted to - you know to be pulled into that direction.

(James Bladel): That's a good point (Dave) and I think that the more we start to peel back the layers of some of these individual comments, the more we start to take a look at some of the - if not language in the report, then deliberations we've had in previous calls and meetings. And I think that you know we should be mindful of our goal, which is to kind of push towards putting a wrapper around this particular working group.

You know whatever that outcome would be, we want to obviously - we want to take all the time necessary, but we should always try to keep it moving in forward and not going back and reopening some of those issues that you correctly pointed out we kind of reached a consensus that there wasn't a clear cut solution. So we - I tried to identify in the report and go forward from there. We want to maybe stay away from those circular topics.

Of course, we're open to the possibility that one of these comments may actually be like a bolt of lightning and cause us to revisit those with a different perspective, and I think that you know there's definitely some potential for that in this group.

(Avri Doria): And there may also be the small stuff like they could contact (often bought with stolen cars). Now I don't know if that's particularly relevant, but I don't remember us ever talking about (stolen cars) and whether that's any sort of additional - that may be, but it's really the due diligence and looking at it and saying, "Yep, yep, covered, covered, covered. Oh, maybe not," you know. I need to go (and look) before I talk more.

(James Bladel): Just looking - it looks like we're starting to kind of approach our - or reach our time here.

Man: Would it be worth sending comments on various items as they are categorized to the list or is that something you just want to keep doing on the calls or...?

(James Bladel): Well I was going to - that's a great point. I was going to throw that out to the group. It's that could we set ourselves a goal and everyone - I

know that (Dave) and (Avri) have already volunteered to take some of the work off list. But can we volunteer to assign ourselves some homework as a group to work through the items that are listed here in Category 1 on the list and be ready to discuss the categorization of where they fit into the report and what the view of the working group is. Whether they were sufficiently covered in the report or whether they warrant further and new or reopened discussion.

If we targeted Item or Category 1 for this next week, then we could come to the call and have a - start to make some determination of where the support lies for these different ideas, and then we can reopen for Item 2 and possibly 3 during our next call.

What does everybody think of that approach? Recognizing - I should qualify this that if it sounds like I'm winging it a little bit, I am. We're really just trying to kind of get this - keep this thing moving forward and make sure that we're being thorough in touching on all of these different comments and making sure as (Avri) said that there isn't some small mention, or sentence, or idea that we completely overlook in this process. And we need to get it incorporated into our report.

(Avri Doria): It seems to me a good approach to get you know a first stab on each of these things that server as - you know the (bit of words) that we beat on in the next meeting. You know so that somebody volunteers to say like, "I can take the 1(H) and say something." And then that would be a good starting place (to help us say), "No, you are completely wrong, et cetera." Then you know you do have a starting place to go from.

Man: Can I ask a question just in the interest of getting things done? Are we under an obligation to address every single public comment, or are we

under an obligation to review, pick the ones we think are important, and say something about them?

(James Bladel): I think at a minimum - if there's a comment, at a minimum we should say, you know, "We acknowledge the comment." I think we are under the obligation to acknowledge comments, but not necessarily respond to them.

(Avri Doria): I think that the staff in their new (GCLD) process did set a fairly decent standard of looking at questions. Certainly when you have five or six questions that can be categorized as the same comment, then you can answer those with one answer you know and such.

But I think that there's a - one of the comments that we've often gotten from people in the GNSO Council is that you don't take (community comments) seriously enough. And I think one of the things that we've decided to try and do -- and as I say, the staff gave us a very good example of it in the new (GCLD) process -- was yes to take each comment seriously, to group them when they can be grouped, and to address each and every issue in some way.

And I do believe that you know - so it's somewhere in between what you asked. Do we need to answer each one individually? I don't think so. Do we need to have taken it into account?

Man: So if the groupings look good, then the least we have to do is address the groupings of comments.

(Avri Doria): Yeah and there would probably be various standout things that you know we (wouldn't) address. So yeah, there could be a base comment

to the group - a base response to the group of issues and then you know - and then some specific things brought out. That would be one way to approach it.

(James Bladel): I agree, (Avri). If there's - if there are those comments that are a new discussion or take our deliberations in a different direction, then we should definitely highlight them and respond to them. And possibly if it's appropriate, even reach out to the commenter.

And I've seen in the past other working groups have invited folks to post to a list or to participate on a call on a guest basis. I think all of those are options that are on the table. But if we find that there are several comments that have a lot of common elements and are thoroughly addressed in the report or can be addressed with minor changes to the report, then we can address those as a category while acknowledging the - that they were part of a group of comments from individuals.

So one way to go forward here for the next week is to - there's two options I can think of off the top of my head. One is that we as a group attempt to respond to the different items in Category 1. Another way would be to solicit volunteers and/or inductees to take individual items separate and then report back to the group. I guess we've already got a couple of volunteers for Item and Item H. Do we have anyone who wants to volunteer for or a group of folks who maybe want to volunteer for those B, C, D, E, and F that are a little more - have a little more common elements.

Or we can - obviously, we have no (standing) to make assignments, but we do want to keep this going. I think that if we leave this open

ended, there's a very real possibility that we could come back here next week with just a couple of these addressed and a lot of holes in Section 1.

Man: Is there consensus about the two extra columns in the comments section - essentially the view of the working group and how we are to incorporate. Are we in agreement that those are the right things to have essentially there as a report?

(James Bladel): No, I don't think that's necessarily been settled, but I think that we definitely want to focus on Column 4 at this point - how and where to incorporate it into the final report or whether to incorporate into the final report or whether it's already addressed in the final report. I think what we're looking for here is an assessment or an analysis of the comments as individuals and say, "You know is this sufficiently addressed? Are there new elements raised? Is this something that we feel that the group may have possibly overlooked in its earlier work?"

But I don't think that those comments are set in stone at all. Columns, I'm sorry. Not comments - those columns.

(Avri Doria): They seem useful. They seem like things we have to deal with.

(James Bladel): I think so too, but there could be - I guess there could be more. Is that possible?

Man: I guess my concern is just with the final column. In many cases, the comments that are there are actually things that are already in the report. So I guess my suggestion would be to sort of rephrase that last column as is this already addressed in the report. And if not, where

should it be added if it is going to be added. But in many cases, I think some of these comments are already there.

(Avri Doria): So one could be if/how/where.

Man: Excellent approach, yes.

(James Bladel): Yeah, I think that's a good approach. Any opposition to that?

Okay, I've already taken us almost ten minutes beyond, so I still wanted to focus on any volunteers or a group of volunteers to - and we're going to take (Dave) and (Avri) off the list since they've so graciously already thrown their hats in the ring through our deliberations. But any other volunteers for remaining items in Category 1?

(Joseph St. Sauver): What I'd like to go ahead and do is just take a shot at sort of seeing if I can peg where each of them basically fit and probably just provide a real terse comment or two for each of them because there are not actually all that many of them.

(James Bladel): Okay, I'm sorry. I'm having trouble recognizing voices. Was that (Joe)?

(Joseph St. Sauver): This is (Joe).

(James Bladel): Yeah, okay. I appreciate that and then I will go ahead and volunteer (Joe) to work with you on that. We're talking all of the items in Category 1 except for A and H, correct.

(Joseph St. Sauver): Yeah, what we want to go ahead and do is just provide a very brief kind of response to each of them. So essentially, if it's a one-line comment, I don't think we want to have a two-page response.

(James Bladel): Oh, exactly and I think there's a lot of commonality there. And then the other open question I think that was possibly raised by (Greg) was that 5(A) should be moved into Category 1. Was that (Greg)?

(Joseph St. Sauver): I think that might have been me again. Sorry, this is (Joe).

(James Bladel): Okay, yeah. Okay, (Joe) so perhaps we could include that as well.

(Jose): It seems to me that - this is (Jose) from (Arbor). It seems to me that both 5(A) and 5(B) could easily be fit into one.

(James Bladel): I think that's a good point. So why don't we because again we're over time. So why don't we just take that approach of tackling Item 1 and I would just encourage folks to please monitor the list and stay active. And if you have contributions to make or want to throw your hat in for some of these other issues or if you feel strongly about one of them or if you feel that perhaps it's not getting the attention that it deserves and it needs to be in a different category, all of those items - please state so on the list.

And when we get together next, we can start to take the temperature of the group and see where we're at as far as support for the analysis.

The question I have is (Marika) is this our new timeslot now or are we just going week to week with a different (doodle)?

(Marika Konings): We hope that this is the new timeslot. There's only a conflict next week. So I would propose to have the next call in two weeks' time if everyone agrees with that. Otherwise, we would need to send out another (doodle) to find a time for next week. So if there are no objections, I would like to propose to have the next call in two weeks' time at the same time, same day, if that works for everyone.

(Joseph St. Sauver): I'm not going to be able to make that one. This is (Joe).

(Jose): Fine with me. This is (Jose).

(Ihab Shraim): Fine with me. This is ((Ihab Shraim).

(James Bladel): With the expectation that this is an every other week call, then that possibly opens the opportunity for us to get more accomplished in the interim. So I would just say tuned to the list. We will try and get Category 1 addressed before our next call and possibly open up the discussion on the list on Category 2, which is a very thought provoking topic.

(Marika Konings): And (James) just to clarify, I think the conflict is only there for next week. So if people in two weeks' time feel that they want to have a weekly call, I don't think that's a problem then.

(James Bladel): Okay, maybe we can then put that as our first item of administrative housekeeping before we dive into the material of the report or the comments so that during our next call we will discuss how we want to go forward from there.

Glen Desaintgery: This is Glen and I'm hearing you correctly. We are going to skip the week - we are going to skip the 15th of April and then we plan to go onto the 22nd. Is that it?

(James Bladel): Yes, that's correct. You know for those in the U.S., it's a tax day and having a (Fast Flux) meeting on that day is just kind of you know compounding the...

Glen Desaintgery: Is that the 15th - is tax day?

(James Bladel): Yeah.

Glen Desaintgery: Okay.

(James Bladel): So we would hate to do that to folks.

Man: I'm sure there will be plenty of (Fast Flux) attacks on irs.gov during the next week for us to study too. Yeah, well one of the things that some of the phishing and fraud scams do is try to get people to disclose their personal information by claiming - trying to be the IRS. And there is something wrong with your tax submission and, "Oh, your e-file information is incorrect. We couldn't route your refund to the bank number you provided. Please log in and give us a new bank number."

Glen Desaintgery: Oh. Oh.

Man: It's not just the United States. You know Her Majesty's revenue you know in England is equally beset. It's pretty ugly.

(Avri Doria): Well I still do mine on our (own), so what can I say.

Man: I'm going to put my money in a mattress for now on.

(James Bladel): Okay, well with that, let's conclude the call for this session and we will reconvene in two weeks. And of course, there should be numerous action items and activities on the list.

So thanks to everyone for participating. This is probably the best turnout we've had in several weeks. And I'm excited about...

Man: The time is good.

(James Bladel): Kind of resetting this group and getting a thorough analysis of these comments and getting them into our final report and turning that over to our council.

Man: Thank you very much.

(Avri Doria): Thank you so much.

Man: Have a good one.

Man: Thank you.

Glen Desaintgery: Thank you.

END