Fast Flux PDP WG Teleconference
TRANSCRIPTION
Friday 18 July 2008 15:00 UTC

Note: The following is the output of transcribing from an audio recording of the Fast Flux PDP WG teleconference on Friday 18 July 2008, at 15:00 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-fast-flux-20080718.mp3
http://gnso.icann.org/calendar/#jul

Participants
Mike 0'Connor - WG Chair CBUC
Mike Rodenbaugh - CBUC - Council liaison
Zbynek Loebl ISPCPC
Ry c:Adam Palmer - PIR (registry constituency lead), Greg Aaron – Afilias, Christian Curtis – NCUC
Registrar c: Paul Diaz – Networksolutions, Eric Brunner - Williams – CORE,
James Bladel - Godaddy
Wendy Seltzer - ALAC liaison ICANN Board
Observers - (no constituency affiliation) Dave Piscitello - SSAC Fellow Randy Vaughn Marc Perkel Rod Rasmussen - Internet Identity APWG Joe St. Sauver - Oregon University

Staff:
Liz Gasster
Marika Konings
Glen de Saint Gery

Absent:
Kalman Feher - Melbourne IT - apologies
Rodney Joffe - Neustar - apologies

(Mike): I'll get the agenda in front of us since we - are we recording now? Not quite yet.

The rules of the road on recording for those of you who haven't been on one of these calls before is that these calls are recorded and the recording is published to the Net and they're also transcribed. And that transcription is published to the internet as well so. One of the conversations that we had during the email was the question about private and sensitive information. This call is probably not a good place to share that kind of information. That's just my little ProForma statement.

I can't tell if we're being recorded yet. (Glen) can you see that on the meeting thing whether we're being recorded?

((Crosstalk))

(Mike): Say again.

The recording has just started.

Woman: Excuse me Ms. Desaintgery has now joined.

Woman: Sorry operator is the call being recorded yet?

Man: Hello.

(Mike): Hi gang. I'm multi-tasking, (Mike) here. We had a couple of folks dropped in.

Woman: Hello? Excuse me, Ms. Desaintgery is starting.

(Mike): Hey how are you doing?

(Mike): We're just sort of settling in. Getting folks on the call and getting into Adobe connect and we are being recorded now.

(Mike): Yeah. Usual rules for sensitive and private information pertain. The call will be posted to the Net. And I think we'll start.

I've got - I hope you can see the agenda in front of you on your screens. Is that what everybody sees right now? Somebody just cheer me up and say yes.

Man: Yep.

Man: Yep. (Unintelligible).

(Mike): Because I've got three monitors and I'm just hoping I'm broadcasting the right one. So I sent this out just a half an hour ago so for those of you that haven't seen this it's because - my bad, I meant to do this last night and forgot.

But I thought what we would do today is take a very brief tour through the action items that we had from last week. Also very briefly skim through sort of my transcriptions of the very - I don't know, I can't come up with a good word but I thought that the email conversation this week was terrific and I have pulled pieces of that out and (sprayed) it up into the wiki and I want to give you a tour of that and get some feedback on that.

Then we've got some topics that I think would bear some discussion and could help us, you know, it's not that we're exactly stuck but we've got a lot of work going on in the email list on these topics and I think it would be just useful to spend some time together on the phone talking about them. I think it's useful to have two forms of communication sometimes.

And the two that I picked out are - are the definition of Fast Flux. We've been having quite a conversation about that and also the whole what

kind of data do we need and is this a problem that needs to be solved. I'm sort of making that a rhetorical question and would welcome other topics that people are feeling the need for some conversation about. And then we'll do some planning for next week.

One of the things that I'm going to start doing which I also just realized that I should be doing and didn't is as of next week I'll start doing status reports that are just very simple status summaries of the things we did this week and what's coming up and we'll go through that in subsequent calls. But I haven't prepared that because it didn't dawn on me to do it until about 10 minutes before the call.

Does that seem like a good agenda? Is there anything that people are feeling the need to add to that? We're going to try and keep it to an hour and a half, two hours felt a little long last week and so we'll try and end in about an hour and a half instead of going all the way to the top of the hour. But if there are things that we need to add, this would be the time to do it.

I'm going to also try and keep an eye on the hand raising and use that as the queue but I may fumble a bit at the beginning because that's a new part of this system that I haven't used before so if I goof that up, just let me know. But if you want to get in the queue, raise your hand on the - on the Adobe connect thing and I'll see it on my screen.

I'm hearing no additions to the agenda so I'm going to take us off to the action items and the first one is just to sort of review where we're at on the questions and we're actually doing pretty well on the questions. We gave ourselves the task of sort of doing these first six questions and the sort of easy queue is that if there's a Web page under here, we've

gotten a start going. And we've done three out of the six but that darn (Dave) wrote such a good response on the first one that, you know, I'm not feeling a terrible amount of pressure to finish the last three although I think that (Eric), somebody is thinking about writing one for the registrars.

Man: (Eric).

(Mike): Is that right? And I'm sort of looking forward to that because I think that one unlike some of the others is - is going to be very important for us to take a look at pretty hard so. I'm looking forward to seeing that one.

But in general I guess as sort of a summary I thought we made an awful lot of progress and covered an awful lot of ground, and covered ground beyond the six questions pretty well. So I - I'm feeling pretty comfortable about that and that's about all I've got to say about those right now. If people want to start drafting the other two, by no means let me stand in your way but I think we're doing really well on that.

We had another action item to reach out for some actual data about the prevalence of Fast Flux, the impact of Fast Flux. We handed that one off to (Dave) and (Greg) and to - I can find that...

Man: (Rod).

(Mike): And (Rod) yeah, there we are. There are those action items. And I was curious how we were doing on that. We got some data and I'm going to go through that in a minute but it didn't come through that channel. It came really more through the email so (Greg), (Rod) any - any thoughts here, let's see. Who got their hand up first, (Greg)? Or

(Randy)? I don't know, I'm going to take them from the bottom so (Randy) first.

(Randy): Hi I'm actually trying to enter the room here so…

((Crosstalk))

(Mike): I'm sorry. Yeah, old guys with bad glasses.

(Randy): Hey.

(Mike): My fault. But (Greg) raised his hand so (Greg) did you have something you wanted to add?

(Greg): Yeah (Dave), (Rod) and I have been drafting a pretty detailed note that we're - we're ready to send out the anti-phishing working group general membership lis - list. So that goes out to probably over 1,000 entities and multiple companies. And lot of - I think we're done. I think (Dave) gave his okay.

(Dave): Yeah I got his final edits there and in the process of putting that out.

(Greg): Okay and I think we've all done a little bit of individual outreach. I've reached out to (Monaxey) group to Indiana University and as a result she decided to join us I guess.

(Mike): Yeah, she's on the call.

(Greg): So I think we're - we're good to go.

(Mike): Cool. Well that's great news and when do you think that (Echo) will come back from the - from that note to the working group? In a week or so?

(Greg): What do you think (Rod)?

(Rod): I imagine we'll get some in right away and I - I would think we'll probably get data for several weeks but hopefully most of it...

(Mike): Certainly sounds like we'll have a good chunk of data before we get our (unintelligible) which is terrific. Cool, that's very good new. Thanks.

(Rod): There's - there are a few people we've kind of preceded, they know it is coming. Yeah they're ready (unintelligible).

(Mike): Great.

(Rod): What we're trying to do is try to get the things in the same format.

Man: Having a real hard time hearing that.

(Mike): Yeah, (Rod) you're awful far from the phone. Maybe you could either get closer to the phone or kick the volume up a little or something. Or shout - shouting's good.

(Rod): Is that better?

(Mike): Oh that's way better.

(Rod): Yeah, I was just saying that we pre - preceded some - some folks that already have lots of data with the idea that the request is coming. We've just trying to make sure that we get something fairly uniform from people so gave the debate over the week with the parameters and things like that that we wanted to collect and ask for so we can actually get data that we can compare at least somewhat apples to apples.

(Mike): Oh I see. This is sounding like it's going to be great stuff. That's terrific. Okay thanks for the update on that one. We had another action item to reach out to legitimate users of Fast Flux and I am winding my way through the hallways of Thompson Reuters because I know the COO there and he's putting me in touch with sort of the right folks but I haven't hit anything yet. Did any - (Wendy), (Eric) did you all have any luck reaching out to some of the folks that you were thinking of?

(Wendy): (Wendy) here. Also working my way through to - to try to follow up on some things that I've heard but still working to confirm.

(Mike): Okay.

(Eric): This is - this is (Eric). I spent my week moving and dealing with a lot of emails. I'm not sure that we should actually try to find a - a good sample because it may be very difficult to find a good sample. I think we may reasonably, simply hypothesize the system of reasonable instance of pervasion that doesn't involve material benefits in the form of money through the offer of it - fraud basically or any of the other schemes we have discussed that need some vague (unintelligible) for legitimacy.

(Mike): And that came up in the email conversation. And - I'm typing and talking at the same time.

(Eric): Right.

(Mike): Sorry about that. Let's - let's defer that conversation for a moment in the call.

(Eric): Fine.

(Mike): I want to add that to the - this is part of the definition of Fast Flux discussion, oh (damn) - were we had a fairly spirited off list conversation about the definition of Fast Flux and I think that hypothetical, legitimate user bears on that conversation because it's the whole question of whether Fast Flux includes the use of botnets that were captured illegally, blah, blah, blah, that whole conversation. So I - I get that and I think that's a great part of the definition of Fast Flux conversation that's coming up.

Okay I - I do want to kind of push it through these. Anyway I think that we're doing fine on our action items. I don't think we have anything outstanding and are fine enough to clear that part of the agenda. I want to just give you a tour, don't actually want to go through these in any review kind of sense but I want to give you a feel for what I've been doing. And - and I will tell you that I've been learning as I go so I'm not - I have no editorial pride at all about what's up on the wiki so far and I figured out that what I need to do in the future is post this stuff to the wiki as it goes by in email rather than being lazy and waiting several days because I then had to go back through a couple hundred emails and I'm sure I missed this stuff. And I won't do it that way this week.

In terms of the (who) benefits I basically have to kick hats off to (Dave). He got first up on the board and I thought he did a fabulous job on this impact statement. And in fact it's such a good job that I started to get a little bit laid back about some of the other subsequent questions because I sort of felt like we at least got the beginning of an answer to some of these.

The - the winner of the longest most words in a single post award and good stuff too. I don't mean to belittle it, it's just that it's a lot.

(Joe): Yay.

(Mike): This isn't yours this the registrar impact. This is the one that (Dave) wrote for me so (Dave) gets another gold star because I started a thread that basically said I don't know and (Dave) came back with this so this got up on the - on the boards. Thank you (David). But here I'm going to bring you to (Joe)'s. (Joe)'s is the champion. Longest internet users how are they affected and I - I will just scroll down, I won't let you read it. You're all welcome to read it on your own. And I started viewing this the way I - I view the sand before we start doing sand sculpture. And I will go through this and - and edit it a bit but, you know, (Joe) got the most words in a single post award and - and good stuff too, I don't mean to belittle it. It's just that it's a lot.

(Joe): Give me a word count for the next article, I'll go ahead and keep to it.

(Mike): Well, you know, the email conversation has been just a blast. I've been having a great time and, you know, thanks to all of you for all of this stuff. I think one of the things as a report writer that's, you know, it's

much preferable to have too many words than too few. It's really much easier to thin out something than it is to sit around and have no conversation and no forward most of them near or far from that.

The other thing that started to emerge until I started just posting things in the wiki is technical changes and policy changes. And I started just scooping things out of the email conversation as they went by and posting them out just pre - pretty much arbitrarily dividing them into technical and policy changes. But again I have no editorial pride here at all and I will continue to do that this week as we carry on with the email conversation.

But this is the point at which I sort of throw my body in front of you and say don't feel like this is my wiki that only I can edit. Feel free to go in and change any of this stuff, comment on it, so on and so forth. And as we start to migrate out of the sort of intense brainstorming that we've been doing (over) email, you know, I certainly don't feel like I want to be the only author of the wiki. I'm happy to continue to do it but at the same time I really want to invite you all to join in.

Anyway there's - there's the beginnings of pretty interesting group of possible changes. We're going to have to figure out a way to evaluate these and rank them and so on and so forth but I'm not going to try and do that on this call. I - I really think we've got a couple of key issues we need to discuss and then that will inform some of this other stuff. But I think starting next week we will start being able to essentially treat this as the beginnings of a draft of our interim report and start editing it, adding, enhancing, taking out so on and so forth so anyway there's a lot of activity there and I commend this part of it to you to review and react to and refine.

As things were going along two additional topics came up--oh no wait a minute--there's also a best practices thing that started to show up and I am going to - there's only one and this is where I stuck my little risk management picture. And I am going to take a minute to just advertise my little picture and use this as a way to maybe shed a certain kind of light on the - on what we're doing.

I - I know that this is not the end all and be all and I'm certainly not purposing this is our methodology but when I've been watching the email, we've had a lot of conversation about the value of this kind of data. Compliance and activity monitoring sort of data and I'm really delighted to hear that we're making such good progress with (Greg) and (Rod) and (Dave) on getting some really good data coming back maybe in a consistent format. I think that will really inform what we're doing. We've - we've also in a way then identifying stress, figuring out what's going on and vulnerabilities, you know, a lot of that conversation in email has been up in here and - and the - the interesting debate for me is in the middle.

I don't think we're ready really to make this choice but I want to just highlight the fact that there is a choice which is that in any sort of risk situation you ca - you can range from the extreme of saying this risk is small enough or has a small enough impact or is likely enough that I'm just going to assume it and ranging all the way to the fact that this rik - risk happened so much and it's happened so often and it's so predictable that I'm going to go buy insurance.

And somewhere in the middle is where risk managers make a lot of money figuring that out. And I think that one of the things that we can

do in the workgroup that will be very helpful is to sort of have an interesting debate about this a little bit further down the road. Once we've done a bit more in identifying assessing part and have some data to look at. And at least for me I am not - I don't have an opinion yet in the middle. I - I don't know what we should do. And I would hope that we would all sort of stay open minded for a while yet on this until we've got some of the data that we need and a little bit more detail on what the threats are and also some of the possible solutions that - the solution set that's emerging is quite interesting I think. And some of it is pretty low impact, pretty low cost. Some of it is pretty high impact, pretty high cost.

And I think that once we've got a little bit more information on the top and the bottom that's when we can come to this discussion and figure out really where we want to land as a group. So anyway that's my little rant about risk management. I won't bug you about that ever again. I'm going to promise. But it's been helping me as I've been thinking about this.

And that - that sort of concludes the tour. What I want to do now is I want to zero us in on two topics that I think are - are really important. I - it's - the one I would really like to beat up today is the question of what definition we want to use for Fast Flux. Hopefully you all can read that, it's out on the Web site feel free to just use the Web site that is if it's too small or too hard to read.

The initial definitions I think I listed from (Dave) or the report, I can't remember now. And the - the debate I think has been really constructive and I - I just want to kind of let us retrace that, you know, I know (Dave) was sort of getting to the end of his string yesterday but,

you know, I hope (Dave) we haven't lost you on this one because I think this is one that needs to get driven in now to a good solid definition that will help us all. It'll help go out for data, it'll help define our decisions, etc., etc.

And so you can see a bunch of clarification that I just scooped off the email and I think that the one that has started to help me is I think the very last one. (Joe) is on the - on the boards for this one and was - was it (Greg)? Who had the sort of the other side of this conversation in the email? Can't remember who? (Greg)?

(Greg): Well hi. This is - this is (Greg). I don't - I don't think there's an issue of the - we - we all agree that botnets are usually composed of Zombie's that were not consensually created.

(Mike): (Correct).

(Greg): The - what I - what I did in an attempt to provide some more material for discussion into kind of just (buying) the issues, I - I then posted some notes below that actually you'll see if...

(Mike): Oh.

(Greg): you scroll down. And - and what I did is I took the definitions from the - the issues report and posted those and posted the definitions from the (S-Act) report. Each of those papers had a definition section and then - and - and they say congruent but the issue is that the - the lingo in the security world is that Fast Flux means the - the use of the DNS with criminal purpose. So, you know, cloakal - cloakal we're talking about Fast Flux we're really talking about people who are using it for - for

crimes or abuses. Now in - in the issues reporting and (S-Act) advisory there are actually distinctions between the - the technical implementation which might be considered (unintelligible) value mutual. And the intent for which it - it is - it is employed. And that's - that's what I was trying to get at.

And the - the thing that I'm trying to get a handle on is there might be uses of the technique or the technology that are not necessarily criminal and we've been - a few of us have been turning over an example and trying to make (unintelligible) of it. So I put some material up here in attempt to - to lay out the issues and invite some - some commentary. I think either were missing a term for non-criminal (users) or we don't know what the original intent of the term was. I - I don't know.

(Mike): (Christian)?

(Christian): It seems to me for our purposes we're probably not really going to be able to effectively address uses of the technique based on the intent. And that - so that we as in our analysis really ought to rely more on the - a definition that doesn't take intent into account because that might lead to sort of a deceptive disconnect between, you know, when we're talking about addressing the problem and talking about what the - the impact will be in terms of legitimate use.

(Mike): (Wendy) I saw your hand go up, do you want to chime in?

(Wendy): Yes, very much the same lines that I think we - we need a generic definition of the use of - of rapidly changing DNS records without reference to the intent - to the intent and then can narrow it to what -

looking at one class of those uses but often we won't be able to figure it out or as we've seen in some of the discussions of legitimate different vantage points will see different conduct as legitimate or illegitimate. And so we should at least start from the value neutral perspective.

(Mike): Well and this was the - this was sort of why I was in trance with (Joe)'s idea that maybe a fingerprint that we could put into this which would be value neutral is - if machines were hosted on bots that have been obtained criminally that that's Fast Flux, but if they are not then they are not. I'm curious if that works. A way to fingerprint Fast Flux the bad behavior from Fast Flux call, you know, call it something else that's legitimate.

(Christian), go ahead.

(Christian): It - it seems to me that - that distinction is only useful if the remedies that we're purposing is specifically limited to instances where we can identify that - that it has been created through a - a botnet.

(Mike): Expand on that a little. I'm not sure I follow you.

(Christian): I guess I - I'm thinking that our definition is inherently (unintelligible) the value of our definition is inherently linked to whatever actions that we're going to take because what we really want to know is not, you know, what's the extent of the malicious use or - or, you know, who would be harmed if - if this - this practice were - the malicious uses of this technique were - were eliminated it's more a question of what's going to be the impact of whatever options we're looking at. And what is going to be the - the - so if we're looking at something that's going to

say categorically label anything with a short TTL that's not registered as, you know, fraudulent or high risk then, you know, we want to consider what that means for - for all the uses that will be best labeled. That - that make sense to you?

(Mike): I am - I'm not - I'm not sure. I would hate to write the note of that. Sorry to be so thick. (Wendy) if you're tracking since you've got your hand up do you want to try and restate what (Christian) just said and then led into yours? If not, I'll - I'll try again.

(Wendy): I'm not sure - I don't think I could restate what (Christian) was saying. I wanted to just add a different thought to the mix so maybe I'll wait.

(Mike): No, go ahead, as long as I've disrupted (Christian). We'll come back to you in a second, sorry.

(Wendy): Well my concern is put - that putting criminal into the definition assume it's the measures that we propose as responses will be able to determine the criminal nature of the activity. Already that seems to me to be looking a couple of layers too deep at the activity going on.

(Mike): So maybe my fingerprint isn't such a good idea huh?

(Wendy): The - it's great for - for law enforcement who are looking at the problems to - to say this is what law enforcement should be focusing on but for our purposes within the ICANN context I'm not sure how we could possibly craft something that was useful and responsive to - to the criminal aspects of activity.

(Mike): I - I wasn't even thinking of it so much as - as criminal and, you know, let me just roll back up, sorry to bother your screens here folks but I'm going to just roll back up to (Joe)'s. (Joe) says sort of mostly criminally but he's really landed hard on non-consensually and by now we're in (unintelligible) all the rest of that highlighted sentence at the top there. Does that side step the criminal because I - I tend to agree we are not in a real good position to determine criminal behavior for sure. (Christian) go ahead.

(Christian): I - I - I think that it's - well it may somewhat side step the question of what activity is criminal and what is not it still leaves us with the problem that we - that only a useful distinction were able to determine what is non-consensual and what is not.

(Mike): Yeah, that's true and I - I think that the short hand for that at least in my mind was that if it was a machine sitting in the middle of Comcast Broadband user IP range that it's probably likely to be non-consensual but I wasn't sure if that fingerprint could be improved or not.

Woman: (Unintelligible) will be happy to join in the network serving up information to dissidents.

(Mike): Yeah, yeah, yeah, okay, okay.

((Crosstalk))

(Mike): Dang nabbit. Okay so what do we do folks I mean how can we get to a definition that let's us sort of go forward in the right way. (Greg)'s got a bunch of stuff on the screen. Can people read this or is it just so small that you're - you're basically seeing a blur? Go ahead (Mark).

(Mark): Okay one of the things I was thinking of as far as definition of criminals there might be something like a universally criminal thing that we could all agree that bank fraud is criminal that - that child porn is criminal but other things are, you know, marginal or something like that. There's certain types of activity and methods that are criminal like using people's computers without - without consent, you know, would be criminal.

(Mike): Well that's the thing that I was intrigued with was the non-consensual but, you know, there is the question of well how do you determine consent and I don't know if that puts us in a box or not.

Man: I'd say one way if the doesn't know their computer's being used for that that would not be consent, you know, maybe that would be a - a better definition than saying, you know, what exactly is criminal or not criminal but I - I like your consent slant on it. It - it's probably the definition anyhow, I - I think you're on the right track.

(Greg): This is (Greg). Believe it or not I found out that there are opt in botnets.

(Mike): Oh great.

(Greg): And - and analyst's have tried (Man Tech) and other places have written about these. I don't know how many of them there are. Some of the - some of the uses are fairly innocuous. People use them to - to - to bomb online polls so there party comes out on top. Others are actually used for (d dot). There's - there's one in the - one out of the Middle East evidently which is - which is pretty nasty. But such a - such a consensual opt in thing exists to sort of complicate things but...

(Mike): But maybe consent is still the - well, I don't know. Let's say we had a botnet that was comprised entirely of people who consented for a minute, would Fast Flux across that botnet be something that we would want to address or would we consider that a legitimate use?

(Greg): Well I mean, like I said one of these botnets are used for (d-dot) which is, you know, terrible. So if - it's an opt-in botnet but it's used for - for that purpose and I don't know if there (unintelligible) used for benign purposes or peer-to-peer stuff, I don't know.

(Mike): Well you know the (Setty) project always sort of struck me as similar to this in a way I mean it's not quite but, you know, masses of computers being used to do a common shared thing. I don't know that (unintelligible). Are - are there folks, I mean, you know, this - there's a reason why I stuck this on the agenda. I'm - I'm stuck, I - I don't know what to do. (Mark) is your hand still up or am I just - I'm just forgetting to get rid of it. (Christian)'s hand went up.

(Mark): I - I didn't get rid of it so you can take - but I would like to say one thing though, you know, we could say that denying other peoples services is criminal even if with the opt-in. And bank fraud is always criminal regardless. So maybe we need to say certain things are always criminal, certain things are usually not criminal and there could be some in the middle that we just don't know.

(Mike): (Christian) go ahead.

(Christian): I - I just want to suggest that maybe we don't need to get (unintelligible) definition as long as we move forward telling that

whatever remedy we look at - if we know, you know, when it's going to impact only those - those - those uses of the technique that we want to stop versus when it might have more - more far reaching effects. I think that's the important distinction that as long as we're able to address that with each technique I think that those words be attached to it are not so important.

(Mike): What do others think? That's the fan. Well I think what I'll do for purposes of today's call is declare us in need of more email about this because I think this is a - I don't know why this is a very intuitive reaction but intuitively I'm feeling like this is important to get resolved. Because if we, you know, this is sort of like in a way describing the destination and if we describe the destination wrong we'll kick ourselves to the wrong place, we'll pick the wrong path to get there. Whereas if we describe the destination well, then we're likely to come up with better solutions. (Rod), go ahead.

(Rod): Yeah, I just want to put even more I guess muddy - muddy the waters even more a bit and if we're going to worry about where we're going to go in general I think that the word fast in Fast Flux is a real problem for us. Mainly because it seems basic techniques are being used by lots of different criminal organizations. But they're not necessarily doing them quickly, they're doing them automatically. Whether it's something in a bot that they're using is taken down, they automatically change but they don't rapidly rotate between them. The most famous example of that would be the Rock Phishing Group where they don't change IPs but all the other techniques are the same. The bogus registrations, the use of compromised servers, etc., etc., etc.

So and I know we're the Fast Flux working group so we have to work with what we started but if we're thinking about how we're going to provide recommendations/best practices or what have you, we'll need to make sure that we have a - a - I think that other u - other types of flux in mind as we're doing this as we go through here so. And I know that could really blow up the definition quite a bit th - and I don't, you know, we talk about that I think initially we don't want to get too far afield but extremely related and we don't want to come up with recommendations that are going to address one very narrow portion of this criminal use of DNS versus - and then - you're then limited to not being able to solve the overall problems that we're looking at.

(Mike): So is it safe to say that we're, you know, that we're really, you know, kind of aside from the word criminal which we've already beat up, I like the notion of - it's - it's the focus on DNS that maybe represents a way out of this. Oh - well - but then - question for the group. If we zeroed in on DNS and left the bot part out - no we can't do that. We've given all these definitions. Other thoughts folks? Anybody see any threads in here that can kind of pull us towards convergence?

Like a - and (Christian) raises an - an option which is maybe we don't worry about it a whole lot. Maybe I'm just obsessing about it and shouldn't but, you know, these issues about what is criminal, what is consensual seem hasty and puzzling to me and things like if we don't have some sort of answer to those questions we're likely to get asked those questions somewhere down the road and not having good answers at that point will leave us not so credible. I hate that. Well more email. Let's do another weeks worth of email and beat on this and see if we can come up with something. (Mark) go ahead.

(Mark): Yeah I was going to say that perhaps depending on what kind of solution we implement the distinction may not have to be determined. You know if we had something that's (unintelligible) and then basically the restriction base solution where we're making Fast Flux not work for everybody then that becomes an issue. But if we have an informational base solution, you know, that helps other people to determine what's criminal, what's not criminal where the information is part of the determination then having us decide that isn't as necessary as if we're going to impose restrictions.

(Mike): I love that. I think that's a very important insight. One of the things that came back through the business constituency list was the whole bromide should we make the - should we fix the problem at the core or at the edge of the network and in a way that ties into what you just said (Mark). Is that a way to finesse this for now is to leave this a little bit open ended, take a look at our solutions, drive for solutions that aren't terribly (unintelligible) more information based.

(Mark): Well I think we need to look for solutions and then see how the solutions impact different constituencies that maybe using just for different purposes. If we had a solution that doesn't interfere with the legitimate uses then it's not a problem that we have a solution that does interfere with it then we've got to look at (unintelligible) who has the solution.

(Mike): I'm going to capture that too. Hang on a minute, I have to. For those of you who are wondering what I'm doing, I'm typing. See all that stuff I'd just show you that stuff. I'm going to put it over here so it's not bugging you. (Unintelligible). That's a good one. Any - any other good ones like that lurking in peoples minds. If not I - I'm ready to leave this topic.

Better, especially with (Mark)'s contribution there I thought that was a good one. Somebody's typing.

Okay the other one that - and (Greg) thanks for adding all that on to the - to the wiki by the way. That was great, that's exactly what I'm hoping the rest of us will do too. I'm sorry that I'm - I'm not watching the - the (cat) side of this, it's just too many things to keep track of at once so, sorry about that. I - I saw your notes long after you sent them (Greg).

I'm going to back us up then to the other one and - and this one may also be relatively easy today. Actually given the fact that there's a whole boatload of data coming in. And so maybe instead of be laboring this one the way I was planning to I - I will wait and let some of the data roll in from (Rod) and (Greg) and (Dave). So I'll just give you a tour instead of it. I have been sort of scraping off back kinds of questions as they've gone by on the list and thrown out some data that - that came in from various places. Including a link to (unintelligible) on your name I'm sorry. There was - (Monaxey) sent a wonderful -- oh for heavens sakes -- a wonderful presentation that I would just commend to you all if you haven't read it. I put a link to it here in the - in the data section.

And I think given the fact that we've got a lot of data coming in I'm not going to spend the sort of time on that in this call that I was planning on. Which means we have more time for other topics that people are feeling the need to discuss because I'm pretty rapidly getting through my agenda here. And I'm about ready to head into plans for next week unless there are other topics that people are feeling stuck on. I re - I know that the email volume is horrendous but the discussion has been really good. It's - it's clear that that's where we're getting an awful lot of

work done and so, you know, I encourage everybody to really dive into the email and, you know, keep that going because that's been a wonderful piece of work.

But if there are things that have been, you know, like that definition one that we just beat on a little bit, are there others things that have been going on in the email that people feel the need to have a conversation about live rather than through the email? Okay I guess not.

Well then I think it's time to plan the next week. My hope would be that we would finish lets see the registrar is one that is coming. I don't know why when I do a quick on something it decides to go edit the dang page. Sorry about that. I (unintelligible) to get back to my home page for heavens sakes. Sorry about this spasing out there. We're - we're essentially right - right on schedule in terms of developing this with initial draft. We're actually doing I think really well at it even thought the wiki may not impress you with its smoothness and glamour. We are indeed getting an awful lot of stuff put up there. Is it the sense of the group that we want to really continue working on the technical and pow - we sort of started on the technical and policy stuff in the email and it seems like this is the - the active part of the conversation so we may as well continue it.

So we declare this week sort of tidy up for first six questions and really hit question seven and eight and nine. That's the focus for the email conversation this week baring general silence which I take is approval. If anybody thinking that's a bad idea this is a good time to talk. Go ahead.

(Mark): Yeah this is (Mark). I - I think we should add, you know, the - the seven and eight here seems to be more of, you know, restriction based solutions, you know, that I - I'm going to focus on the idea of information base solution until somebody convinces me that I'm completely on the wrong track. Because I think that an information based solution might end up being a better solution, you know, eventually as a - because if we can provide information then people out in the real world here, you know, you know, like people like me and the companies and stuff can use that information and respond much more quickly to changes in criminal activity than a policy based board like eye candy, you know, which might take a year or two to attempt to solve a problem that is being circumvented, you know, within hours of when the solution comes out.

So, you know, I'd like to, you know, explore, you know, solutions that provide, you know, the world with information about domains and that information then can be used (unintelligible) collection and bad (unintelligible) collecting and to make intelligent decisions so as to protect, you know, free speech and civil rights, you know, while at the same time restricting fraud and child porn.

(Mike): That's an, you know, lets visit for a while about that. You know what's emerging in the solution set right now is a fair amount of information based stuff. I think (Joe) got a big one on the boards with this one. It's straight out of one of (Joe)'s posts and then I started chopping it apart and it went on the too hard pile. But if - if you look at the rest of this list there are almost no, you know, I - I think it's safe to say that in the email threads there's been a - a fair amount of earning for accurate Whois I think we could certainly stick her hand up to the Whois task force and say us to we think it's a good idea.

Woman: Not all of us.

(Mike): Not all of us. And except for that most of these are permission based solutions.

(Eric): This is (Eric) and I'm on the Whois task force and I'm really hoping never to say that word in the working group. (Unintelligible).

(Mike): Whois?

(Eric): It is just too loaded with very complicated politics.

(Mike): Yeah I know, it certainly is. Its seven years of history. Well I could scrub that out. Do you want me to scrub it out right now? I'll do that right now while we here. Because I just sort of stuck that in, I'm happy to remove.

Man: I would urge you not to scrub it out.

(Mike): Alright, never mind. I'll - I'll - I'll leave it in there as a debate item. But even that is essentially an information based solution. You know one of the things that hasn't emerged in the conversation yet is the whole question of taking down domains and I don't know where to insert that into this discussion or whether it's not emerging for a reason. But, you know, let's talk about information versus policy based solutions at this point just for a minute to get a sense of where the group is at.

And maybe that's another topic for the email this week. I'm detecting another email topic. Put that on my list of stuff to do.

(Eric): Hi this is (Eric). I didn't catch who it was who immediately responded to your question and should you remove Who
is with a - a preference for retaining it.

(Joe): That was me (Joe).

(Mike): There we go, (Joe). Well let's leave it on and we'll, you know, (Joe) one of the things that's - that we're running into here is that there are - the Whois discussion is a very old and rich one within ICANN and I certainly wouldn't want us to get too deep into that topic because it - it's a very complicated discussion within ICANN.

(Joe): I understand that however I think it's also important to recognize the one characteristic of Fast Flux is that it does tend to routinely and consistently use bogus Whois.

(Mike): Yeah.

(Eric): I appreciate that you have your thoughts on that; however, it's still a policy and (unintelligible) problem.

(Liz): Hi it's (Liz). Right now the Whois working group which (Chuckums) it's not a working group it's a study assessment group (Chuckums) is trying (unintelligible) is looking at defining hypothesis for Whois studies that the council ought to possibly consider doing once those hypothesis are fully defined then the (unintelligible) the council will make some judgements about what studies about Whois ought to be further scoped out and priced out by the staff and - and there'll be a next (generation) where they decide whether to do studies on Whois.

There is no pending PDP or policy development process on Whois right now but this issue - this specific issue about Whois that's been pending for since last fall was what further studies ought to be done that would be useful to best understand or to best help guide the council about what potential further policy development might be informed by those studies. And it's an open question about whether any studies will actually be selected by the council or not and if so, which studies might be selected by the council.

So I just want to - yes there sending out several PDPs of (thunderation) of looking at all kinds of questions about Whois ranging from accuracy questions to the kind of perennial policy question that's been challenging the privacy questions about Whois. But there is no pending PDP right now and the - there's a question on the table now is whether studies of Whois will be done and if so which. I just wanted to update people on that so they know what actually is happening on Whois in a separate study group right now.

(Eric): This is (Eric) again and I contributor to that activity and - and again and half of us decided that there should be no further studies and half of us decided that there should be further studies. But they're (unintelligible) was also DNA connection to attempt to find the hypothesis that we're implicit in the claims for studies by the parties that claimed the study should be done. I'll leave it at that.

(Mike): Yeah, you know, I'm going to take authors privilege on that particular line and take it out of the list because I really don't want to walk us into that quagmire. (Joe) I - I get it, I understand the - the issue that you're raising but that's just one that we'll completely, I mean we can certainly

acknowledge the fact that what your saying is true. I don't have any problem with that but I really don't want us to touch that policy issue. We will...

(Joe): Before you delete it recognize that deleting it means that there's going to be more pressure on technical solutions and accelerated tech down because if the Whois data untrustworthy there's no way for criminal law enforcement and (meat) space to go out and touch these folks. So I mean you really have to pick which of two poisons you think is tastier. Either have more pressure on technical accuracy, on technical solutions or go ahead and recognize you're going to need map people to their domains.

(Liz): This is (Liz). I didn't mean to describe the - the other activities and Whois to anyway discourage, you know, if Whois is or isn't instrumental to addressing this concern in some aspect, I don't think it should be neglected just because it's a little bit, you know, radioactive - that's a bad term and I - I because there are other policy concerns implicated by it because that would be putting blinders on this discussion. So I'm agnostic on the result, but just offering that I didn't intend to convey that it shouldn't be just intended to inform the group about what the status of other activities are. And I would encourage you to, you know, pursue your discussions, you know, without feeling constrained by that.

(Mike): Thanks (Liz). (Mark), go ahead.

(Mark): Yeah I just wanted to add that some of the (unintelligible) is of a doesn't require any type of modification to the information available as Whois but just that to have a high speed connected for reading it but,

you know, people like me and the (stem) (unintelligible) that's - that's can access. For instance, you know, I personally would get no information, useful information about who the registrant is because the registrant is going to be assumed to be fake but if I knew the registrar then I might be able to, you know, create an automated email to the registrar that there is a problem with a certain domain. So if I have a domain that I can see this is fraud, this is child porn, something like that then I can create an automated message and say, you know, to two (unintelligible) you know this domain has a problem that you should look into.

Man: Do - do you use port 43?

(Mark): Well the - the thing is that the Whois stuff is far too slow to do what I need to do and I'd need the information through DNS rather than through a Whois type port connection.

Man: Well you can always become a registrar or a reseller which gives you automated access to certain registry information.

(Mark): Well it's still, you know, I wouldn't want everybody who's in the (stem) (unintelligible) business to have to become a registrar in order to get, you know, information. I - I - I think and also the port, you know, the TCP protocol is - is too slow to - to meet the speed requirements, you know, that only a DNS information protocol using UDP would be fast enough, you know, for real time querying and real time reporting.

(Mike): I'm going to punt that one to email. That's a - that's a (unintelligible) conversation to - to continue. I don't want to stop it entirely, I just, you know, we've - we've had a pretty robust (unintelligible) about that and I

think that can continue. And I think one of the appealing things about technical solution is that it does tip toe around some of these radioactive policy issues. So I hope we carry on on that front for sure.

Let's see. I think that the queue is empty. So I'm going to go back to sort of the upcoming week discussion and sort of focus this on continuing with seven. (Mark) your point about number eight is - is noted and I'll - I'll get that out to the group on an email thread how - and I'm going to call it information versus policy based solutions. That'll be the header on the email and we can carry on that discussion. And I think that'll keep us pretty entertained. Now if we keep up at the rate we're going, we're going to have a pretty impressive body of information to sift through by the end of next week I think.

And make pretty good prog - I - I think we could start in the email now trying to drive towards consensus opinion if we can. So as people that are working away through these threads try and see if we can bring them to a conclusion that everybody in the thread agrees with via email. That'll st - I think be a lot easier than trying to drive all of that in the phone calls and kind of carry on from there. Does that seem like a reasonable approach for the week? Are people willing - I guess here's a question. Are people willing to sort of sustain this intense pace for another week or two? I don't think this will last all summer. I don't think we - any of us could sustain it but I think that we'd - we did an awful lot of work this week and if we can continue this I think we're in really good shape. I - I'm hearing silences. Sure, you bet so I'm going to take that as a yes.

Is there anything else we need to talk about today? Where are we at on time? Oh we're getting close to the end anyway. Are there - are

there other topics that people want to bring up, just anything at this stage?

Woman: (Unintelligible) no.

(Mike): Small person in the background. I think then I'm going to draw this one to a close. I know that it probably pains you not to have to spend a whole hour and a half listening to me but I'll put this 15 minutes in the bank. Maybe sometime we'll run a little over.

I'll just take that last couple of minutes to say anything about the way the call went today that bothered you that I can do to improve? Any feedback for me in terms of - also in terms of email conversations, everything else that's been going on, any kind of feedback to your Chair would be a fair game at this point.

Man: I think you're doing a great job. I like the way it's going.

(Mike): Thanks. Well I am too. I'm having a great time. I'm certainly learning a lot. Other? Take that deafening silence as information of my fabulous job and I think with that, I'll call it quits. And we'll see you in a week. (Rod), (Greg), (Dave) if some of that data starts to trickle in, I'm really hungry for it so don't be shy about pushing some of that along and I'm also really interested in the registrars impact statement. That sounds like an important one to me and we'll call it a day. Thanks folks. Have a great weekend.

Woman: Thanks (Mike).

Man: Thanks.

Man: Thank you.

(Mike): Bye bye.

END