Fast Flux PDP WG Teleconference

TRANSCRIPTION

Friday 8 August 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 8 August 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-ff-pdp-20080808.mp3
http://gnso.icann.org/calendar/#aug

Present for the teleconference:
CBUC
Mike 0'Connor - WG Chair CBUC
Mike Rodenbaugh - CBUC - Council liaison
George Kirikos - CBUC

Registry Constituency
Adam Palmer - PIR (registry constituency lead)
Greg Aaron - Afilias
Rodney Joffee - NeuStar

NCUC
Christian Curtis - NCUC

Registrar constituency
James Bladel - Godaddy
Kal Feher - MelbourneIT
Paul Diaz - Networksolutions
Eric Brunner-Williams - CORE

Wendy Seltzer - ALAC liaison ICANN Board

Observers - (no constituency affiliation)
Dave Piscitello - SSAC Fellow
Marc Perkel
Rod Rasmussen - Internet Identity APWG

Staff:
Liz Gasster

Marika Konings
Glen de Saint Gery

Absent - apologies:
Randy Vaughn
Joe St Sauver

Coordinator: This conference is now being recorded.

Mike O'Connor: All right. I sent just a minute ago the link to the agenda. And we're not going to do the screen sharing thing. And I'm going to try to talk less.

So just to quickly spend through the agenda, first thing up is Glen doing the roll call.

Glen DeSaintgery: Okay (Mike) (I'll do that). On the call we have Mike O'Connor, the Chair, (George Kirikos a new member to the group, (Christian Curtis), (Marc Perkel), (Paul Diaz), (Adam Palmer), (Greg Aaron), (Dave Piscitello), (Wendy Seltzer), (Mike Rodenbach), (Ihab Shraim), (RodRasmussen), (James Bladel) and (Rodney Joffe).

And for staff we have (Liz Gasster) and (Maria Konings). Have we left off anybody?

Mike O'Connor: Looks like we're in good shape. Thanks Glen.

I'm going to send out the next item which is the status report. And I'm going to blast through this one really quick because it's all fine. But here's the link to it if you want to review it.

And there's a reason why I'm pushing so fast through all of this kind of housekeeping stuff just because when I listened to the call last week I talked way too much and you talked way too little. Now I'm changing that behavior.

The next item which I want to spend just a few minutes on is the status of a couple of action items from last week. And then I really want to spend most of the conversation today working on the - basically the draft of the report which is down in the screen in the lower right which you should all be able to scroll independently of each other. Let me know if you can't.

But before we get to that I want to talk to the data people and find out sort of how the data gathering stuff's going with the following caveat.

It seems to me that's what's emerged in - especially in (Dave)'s map of things to do is the recognition that this data gathering problem is not trivial and that we may have set ourselves too high a target to arrive at definitive data in this work group.

But that said, I wanted to sort of hear how things were going from (Rod), (Rodney)'s, (Dave)'s and (Greg)'s of the world. So go ahead you guys.

Man: Any particular order?

Mike O'Connor: Oh, I don't know, arbitrarily (Rod) first.

Rod Rasmussen: Okay. This is (Rod). I was just lax all week so I haven't done much data gathering myself other than I'm here to check to use the Internet anymore. But that's what happens with those conferences.

Yes the - I actually do have some positive feedback from the group in Milan, Italy. And they're going to do a (with the) data on what they've got. I don't have (unintelligible), have to get back to them on, you know, tell them again what we're looking for - going to do that.

And actually it's (unintelligible) if it's not too late for them to join. So (unintelligible) a procedural question (unintelligible) in there (Mike).

The other woman that just came up is the (Honey Nut) project in Australia. I've got - they've actually got an online tool and an open source tool for tracking fast flux (unintelligible).

I'm haven't (unintelligible) yet but it is - we want to set up our own little fast flux -- say that right -- tracking system that we can use, you know, ourselves but - if there's a way we could do that. So I'm pretty excited about that.

Other vendor stuff I have not gotten back from the (link). I keep hearing that they're going to do that soon. And then we do have information coming from Cambridge which is supposed to be eminent - imminent.

The (Richard Clayton) researcher there and has a ton of information on this stuff. And he's just been trying to collate it so that it's not overwhelming and actually makes sense.

That's what I...

Mike O'Connor: Oh that's great. Are you on a cell phone today (Rod)?

Rod Rasmussen: Yes I am.

Mike O'Connor: Okay. It was cutting out a bit. We'll accommodate that. (Rodney), how did your project go?

Rodney Joffe: I have some data to send to someone who knows how to two munch better than I can. Maybe an (Joe) gets to do it. But I've got a pot load of data. And I haven't been able to make too much sense of it only because there's so much.

Mike O'Connor: Okay.

Rodney Joffe: So I think - is there something I can send to now who'll actually go do the analysis?

Mike O'Connor: Do we have any data (mungers)? Yes, (Joe) isn't on the call today. He's in...

Rodney Joffe: I guess Dave Piscitello has done some. Would you volunteer (Dave)?

Dave Piscitello: Volunteer for what, for (munging) data?

Rodney Joffe: For (munging) data.

Dave Piscitello: I've got my own damn data to (munge).

Rodney Joffe: So I need some help from someone who can actually (munge) this because I've not succeeded.

Dave Piscitello: Well I guess why don’t you send it to me.

Rodney Joffe: Okay.

Dave Piscitello: And I will see if I can - I’ll see what I can do with it. And if I can’t - what form of it is it in? Can you send it to me in CFV?

Rodney Joffe: I’ll see if I can get it into CFV It may just be tabbed at the moment. So that may not be a problem.

Dave Piscitello: That‘s fine. Tab is fine. I mean anything that I can import into Excel I can probably (munge) or I can get from...

Rodney Joffe: No, no, no. This is way bigger than your Excel will let you. This is too many rows for Excel.

Dave Piscitello: Oh okay. Well I don’t have anything that’s, you know, that’s going to deal with that kind of, you know, tools. I wouldn’t have to write, you know, from scratch and, you know, in BFB. And I just don’t have time to do that right now.

Rodney Joffe: I’m just looking at someone who’s better than me, better than I am with (ork) and (breath).

((Crosstalk)).

Dave Piscitello: Is (Joe) around?

Mike O’Connor: No (Joe)‘s not on the call today unfortunately.

Rodney Joffe: You know what? I'm going to email it to (Joe) in Austin to do it anyway.

Dave Piscitello: (Joe) might be able to do that. The other person that might be able to do it is some people from (April's Tool).

Rodney Joffe: No, you know what? If I can't get it from (Joe) I will just - I'm just going to pull one of my production guys off of what they're doing and do it during today. Because I'm actually going to start it now. I'm going to send it to (Joe) and also give it to one of my guys.

So over the course of the next and 12 hours we'll have the answers from them.

Dave Piscitello: Okay. Yes I'm sorry. I mean I would but honestly I am just buried with other things and I'd have to be writing scripts. And I suck at that to begin with so it takes me a long time.

Rodney Joffe: (Dave), no problem, no problem. I'll handle it. (Mike), I'll have that for you shortly.

Mike O'Connor: Terrific, thanks. Any other - (Dave), (Greg), any data? I kind of want to push us through this.

Dave Piscitello: Well I did post some data and I posted a scatter plot.

Mike O'Connor: Oh yes. Could you repost that with a horizontal axis label? I didn't know what was across the bottom.

Dave Piscitello: It's just - yes, it's just a number of - or it's the 13,889 post.

Mike O’Connor: Oh so it’s by number.

Dave Piscitello: Just, you know, in order to generate the plot, what I had to do was actually try to introduce a random sort into, you know, into a dataset that, you know, that had two columns.

And so the only way to get some sense of randomness was to alphabetize the domain names because I had a domain name and a number of ID addresses that were used in the attack.

So what you’re seeing is these large blobs that sort of show concentrations of called TTL values. Oh I’m sorry, numbers of changes.

So for example there’s a very, very big distribution of numbers of IPs used over a course of the month in the 600 range and in the 1000 range and in the 1500 range.

You can’t really extrapolate from that anything that has to do with, you know, with TTL values. So one of the things I’ve just asked from some other people is if I could get a similar kind of data of that sort of shows the, you know, the TTL values that were assigned to the name servers of the domains that were used in a fast flux attack.

And the only reason I’m doing that is not too sort of find a number that we didn’t say is the definitive number but just sort of actually debunk the myth that there’s only one PTL and if we nail that PTL we’ve nailed fast flux.

Mike O’Connor: Got it. Okay that would be useful to sort of expound upon in conjunction with that chart because I couldn't figure out what the chart was telling me. But it seems like low alphabetical values have high numbers of hops.

Dave Piscitello: That's an interesting conclusion.

Mike O'Connor: Well it seems like it was high on the left side and low on the right side. Those were the As.

Dave Piscitello: Well I could go look again and see what, you know, see how that (chart) came out. You know, if you look at the scatter there's actually low values and high values.

But it does turn out - actually what's very interesting (Mike) is that I just opened up the Excel spreadsheet and in fact it looks like names that begin with numerics which are first alphabetically of course have a fairly high number of -or a fairly interesting distribution of either above 1000 or under 20.

Mike O'Connor: Yes. That's what I was noticing.

Dave Piscitello: It's very strange.

Mike O'Connor: Yes.

Dave Piscitello: I suspect that that's, you know, - actually that's a very, very interesting session. And all that As have numbers over 1000.

Mike O'Connor: Yes. Well that's why I wanted that horizontal access because I was trying to figure out what that graph was telling me.

Anyway, I don't want to belabor this one either. Any other data and news? We're drawing to the close of this one.

Dave Piscitello: Well trying to get this stuff and then (munging) it is very hard. You know, there's a fair amount of nervousness in sharing this information.

Mike O'Connor: Yes. Well and I think that that's part of the reason I did that little caveat at the top of this item. It seems to me that what we've stumbled on is a job that's perhaps bigger and harder than we thought and that it needs to go into our list of things to do rather than things that we do. Because I don't think we're going to be able to get through it in time. And so...

Dave Piscitello: I think that it would be a really valuable to identify, you know, three statistics that we want to get just arbitrarily picking three. But a small number of statistics we would like to get and then asking for that as opposed to asking for terabytes of information and then try to come up with some, you know, some conclusion based on our own analyses.

Mike O'Connor: Yes.

Dave Piscitello: So I think the two that I think would be valuable and I've be looking at our how many host are used typically, orders of distribution of numbers of hosts that are used in fast flux attacks. And that's the one that the scatter plot's supposed to represent. I'll go take a look at that a little more carefully.

The other one is what, you know, people make this assumption that short TTLs are an absolute marker of fast flux. And I don't believe that to be the case. So I'm trying to get some information from some other people that (well) let's at least say, you know, it appears that there are several different (loci) of TTL values that are used and that TTL -and the conclusion would be that TTL values alone is not a sufficient indicator, you know, that our network is a fast flux, you know, fast flux network.

Mike O'Connor: Right.

Dave Piscitello: So is there any - if anyone else has specific, you know, single (things) articulated data that they think would be useful in making whatever case we need to make in order to prove the - or to justify, you know, doing some work in fast flux, it would be nice to just - to post those so we could discuss them and then try to pinpoint a party who would share at least the aggregate result with us.

Mike O'Connor: I think what I'd like to do is let's push that out into either - let's push that into an email thread. Why don't you...

Dave Piscitello: Yes. That's fine.

Mike O'Connor: ...click that one off. And then, you know, I really like your scheme of taking the points that I had jumbled up and re-posting them at the top of your follow-on email with mine inserted.

So let's try and follow that habit. I think one of the habits that we've got to break is these long complicated indented threads like we had going.

And so maybe what we could do is start building a little list of those one sentence datas that I'd like to collect, statements, and just let that build and then post. Does that work for folks?

Take that as a yes. So (Dave), if you could kick that one off, that would be...

Dave Piscitello: Okay. Will do.

Mike O'Connor: Okay. Last sort of thing before we get into the meat of the call today, and that is a reminder that today is the day for that first round of constituency input. And I haven't been overwhelmed with email containing those. But it's not the end of the day yet.

I have to admit that I have done nothing on summarizing the business constituency input except invite the one person who commented, the joint working group. And (George), it's great to have you in the group today.

So I think I'm going to finesse the business constituency one by saying, you know, you don't really have any input outside of the working group at this stage of the game and carry on from there.

But if constituencies have prepared input statements, today's the deadline to get them in. Enough said about that.

Okay now I want to get to basically one of two discussion topics for today's call. And I want to give you a tour of what I'm hoping will happen.

In the lower right of the screen in the Adobe connect gizmo is a copy of the report as it stands on my hard drive at the moment.

And hopefully you can all see it well enough to read it. And hopefully you can all scroll down to the section that's called Available Options which is about 3/4 of the way down the screen. That is a slightly edited version of the post that (Dave) sent and then followed-up on.

I did two things. I took out some of the words simply to make it a little bit shorter so it would be easier to navigate on the screen. And I added a couple.

For example, I added one that's sort of got (George)'s name on it at least in my mind which is the second one which is document the process and determined intervention choke points. And that the question we're trying to answer there is where is the best place to intervene? And I'm going to have to clarify that.

Is everybody at that spot on the lower right screen so that you can see me typing fast flux in here? Anybody who's not, give me a shout.

Okay, I'm going to presume that we're all on the same square. Here's the thought I had. It seems to me that this is sort of the heart of our deliverable and that if we can really hammer on this today and get it right that we've come very close to writing the first draft of the interim report.

There's a whole bunch of other stuff in here which I'm throwing in here as possible topics. But I think that the real key stuff is contained in this section.

And what I thought we would do is have two chat windows up above, one where people can propose solutions to issues which are raised, and the other one on the right. I'm not sure that this is the right way to do this you understand. Just I'm learning this stuff just as we all are. And so I'm real open to suggestions.

But again back to the conversation last week which was 90% (Mike) and 10% you, that's not very good. So I'm trying to get 90% you and 10% (Mike).

One way to do that is to use both our mouths and our fingers to communicate here. And I thought what we could do is - I thought I would just real quickly spin us through the suggested list and then go back and get these fixed.

And if we can emerge today pretty close to a fixed set of these then I think, you know, we've crossed the great divide.

So, just to start off I'm not going to read them. That seems silly. But why don't we just start with the notion that this seems to be a list that's in sequence. It seems like the first one improve the definition has to get done before the fifth one, establish a preliminary false positive accuracy target.

And that what this in a way represents is sort of a work plan for a project. It's probably a work plan for us. And I think it's a work plan that we would probably have to follow in a subsequent PDP. I don't think we can do all this stuff in the time that we've got.

But if we can agree that these are the right things to do, this seems like a pretty a robust recommendation to me.

So there's my preamble. Reactions first to this idea that we essentially come up with a sequence list of recommendations and then maybe draw a line somewhere in this list that says this is how far we are willing to - we're all willing to agree and (consensus) we should go after which we need to take a checkpoint to see what to do next.

Rodney Joffe: How far do you think down the list we should be going?

Mike O'Connor: I think that at least - you know, I have to take my chair hat off and say that from a personal sort of observation standpoint, I'm pretty comfortable up through may be even costs of the tax before we take a checkpoint.

Somewhere in that zone seems okay to me, that when we get to about that point we will be a whole lot smarter about what we're up against, how it can be detected et cetera. So there's my editorial thing. Now I'm going to shut up. Sorry. Others?

Man: Sounds good to me.

Mike O'Connor: Do other people identify sort of a different place on the list to stop than that?

Rodney Joffe: This requirement of the working group, what does it require? They're ready to be based on the…

((Crosstalk))

Mike O'Connor: In terms of our charter?

Rodney Joffe: Yes.

Mike O'Connor: That's a darn good question. Hang on. I'll go look that up.

Man: I was just looking at that and, you know, it's a list of specific questions that we were asked to answer by the council.

Mike O'Connor: What if we came back and said that list of questions cannot be answered in a sufficient manner in the timeframe we were given. Here's our plan for how to get those questions answered?

Man: If that's the best we can do, that's the best we can do. But at least try to answer some of them, you know, to the extent we can. I mean I think we've got enough opinion expressed in a lot of this stuff start (claiming to) consensus right (Mike)?

Mike O'Connor: Well...

Man: Or you're going to start doing that today?

Mike O'Connor: Yes I mean where I'm seeing consensus emerging -- and (Greg) I'll get to you in a second -- is around this list. I'm not seeing consensus emerge around the answers to these questions. And so that's part of the reason I'm so zeroed in on this list right now. (Greg), go ahead.

Greg Aaron: Thanks (Mike). As far as I can recall, the process for the first draft, it's supposed to incorporate and smooth out the opinions expressed in the constituency statements which are now in I guess.

But I don't see how we could possibly take care of all that in a week because there isn't consensus on a lot of the other points.

Mike O'Connor: Yes I - for example, I'm not even sure that we've got a consensus on the definition of fast flux right now. And I'm not sure that we're going to be able to arrive that in a week.

Because I think what we're all just - certainly I'm discovering is that this is a much more subtle thing to define then I ever imagined it was going to be. Others?

Greg Aaron: I think we need to - I mean it'd be very useful to see what the constituency statements say because there's probably lots of - there's probably a lot of good information in there to rely on and then it will multiply, crystallize where the opinions differ.

Man: Greg we're not (unintelligible) statements for a while. We don't even ask for those.

Greg Aaron: Okay, input templates then.

Man: Yes.

Greg Aaron: All right, (Mike), how many of them have come in?

Mike O'Connor: I've gotten none so far.

Greg Aaron: Okay, I just sent you the registry statement template, whatever.

Mike O'Connor: Oh, okay.

Greg Aaron: Okay? So we haven't gotten.

Mike O'Connor: We haven't - you know, today is sort of the deadline day so, you know, people may be treating this end of day rather than beginning of day. But so far, you know, as of this morning I hadn't gotten anywhere.

Greg Aaron: All right. Well I think that would tell us a lot. It also provides probably some meat for the - for a first draft.

Mike O'Connor: Yes, yes. I think that's right. But again I'm not sure we'll be able to arrive at a consensus around any of those...

Greg Aaron: True.

Mike O'Connor: ...in a week. Because I'm still gunning for sort of a week from now to have the preliminary first draft out there and two weeks from now to have it done. Because if we don't do - you know, if we slide that much we're going to wind up blowing out the end date pretty badly.

And that was part of the reason for my despairing note earlier and part of my enthusiasm for a recommendation that looks like the one that's in front of you here which is wait a minute. This is much too big and much too subtle to address in the kind of timeframe that we've been given.

Man: Sort of - I don't know, I've got to just say that my sense is that we need to ask people (group) to express their opinions on really all of the questions that were asked by the council? And those opinions can be parsed out of the email and phone transcripts and put into a narrative form.

I don't think that answering a different set of questions is necessarily a good idea although certainly we can do that as part of one of the other change - especially in response to Number 10 which is obtain expert opinion on - well no sorry that - but anyway, we could certainly find a way to add to, you know, use this list of questions so that it governs - or not governs but (gets) future work.

Mike O'Connor: Well, you know, again I think the problem is that this list of questions is -well I'm going to let other people respond. Does somebody else want to respond to my comment?

Hearing nobody else I'm going to dive in. It's sort of - it partly as your kind of report writer, I have no way to figure out how to get through what is now close to 1000 emails and do justice to the information that's in there. Does anybody have an approach to that?

Marc Perkel: I have an idea (Mike). This is (Mark). What I think we might want to do is move on to the solution ideas. And then when we look at the solution ideas, that might lead us back to some of the definition problems that we've had.

And, you know, we may be stuck on definitions when we don't really need to be, you know?

Mike O'Connor: Other thoughts?

Man: Well (Mike) I've had to do this several times -actually numerous times with the security and stability of (either) committee. So I will tell you that I don't envy your job because I've done it before. But ultimately there's only two ways to do this. One is that you do slog through the 1000 emails because that's the role that you took or you identify, you know, other authors who are going to take one topic and slog through the 1000 emails for that one topic. And it's not an easy task.

Liz Gasster: It's (Liz). I feel responsible for offering even though I don't necessarily feel that I have the means myself.

If, you know, this is just a suggestion if we're stuck. You know, if we push out dates I can probably get some consulting resource to help do this.

So (Mike) I just want to offer that because I feel, you know, responsible for being able to contribute if we can. But we have the same limitation all of you do. So I just want to offer that up. Staff should be in a position optimally to really step in here. And I'd be willing to but recognize it would end up probably being done at least in part by a third party so there would be a time delay.

Mike O'Connor: Thanks (Liz).

I guess the reason that I'm pushing back a little bit is because I'm not sure that those questions can be answered. So we've done some of the things that's in this list of things to do.

Man: I think that's very legitimate to point out, definitely.

Mike O'Connor: So given that, how do we precede?

Man: In other words in response to these questions we can certainly point out further questions that we have and data that we need to really add to them. But we could also ideally just briefly describe the various opinions (directives).

So maybe the best way to do it now is specifically ask the constituencies to put together statements that respond to these questions. Then we're going to have some text to work with.

Mike O'Connor: Well that's I think what's coming in today for the most part.

Man: Well I was - I mean honestly I was not understanding that that's what you were expected to have today from the (group).

Mike O'Connor: Well that was what the template called for. It basically said dear constituencies, here's a list of questions if you have any suggestions of answers to any of these questions. Please provide them.

Man: Right. Well we just haven't done in the BC what we should've done by now. Yes, and that's my fault…

Mike O'Connor: Yes I'm going to...

(Liz): So I think the overall point is right that also it would be very helpful for the constituencies to try to crystallize information and perspectives on these.

Man: Yes imagine (Greg)'s done a very good job of that from the registry. (Unintelligible) that we need to draft text (Mike) that seem to be (unintelligible) circulated around the BC list. But I understood that that was going to be the final constituency. And it is actually.

Mike O'Connor: Well I was thinking of this first round as the gather the text, gather the ideas. And the second round being the constituency reaction to our proposed answers.

For others who've written constituency - the first round statements, how did you (perceive it)?

Greg Aaron: This is (Greg). We circulated drafts amongst ourselves at the registry constituency. We tried to answer the questions. And so we got into some technology discussions about, you know, what registries are able to do and what they can't and so on.

The hope there is that provides some meat for a draft. We also expressed some opinions, figure we might as well do that at this point, you know, bring up issues which are going to need to be discussed. So that's what we did.

Mike O'Connor: Cool. How about others?

Now by that silence can I take that to mean that there aren't any other first round constituency inputs, documents on the way?

Liz Gasster: So it's (Liz). I know like in the case of the registrar's they have a somewhat lengthy process in terms of considering these questions. And it would be good to know sort of where in the cycle they are with the other constituencies who are on the call as well.

It's not unusual. I mean we threw some heavy questions out so it would just be good to know.

Man: Yes (unintelligible) summertime it’s really hard to get people’s attention right now.

Mike O’Connor: Well and I think part of the reason is that. But I think another reason is that the constituencies may be having the same difficulty answering the questions that we are.

Liz Gasster: Good point.

Mike O’Connor: So...

(Paul Diaz): Yes (Mike) this is (Paul).

Mike O’Connor: Go ahead (Paul).

(Paul Diaz): And weighing in for the registrars, we are still working on ours. We won’t have it ready today. But it should be fairly soon. Since this is the first round this is almost more of the brainstorming or preliminary input stage.

The voting rules and the things that kind of take us longer and perhaps some of the others based on our - the constituency bylaws, that doesn’t come into play at this point.

I think for the next round whenever we are asked to as a constituency formally comment on a draft report that would include proposals and whatnot, that’s the one that often takes longer.

And basically the timeline works out to about a month from first receipt to at least a month I should say to get a response out to the hosting time and then comment period and then a second posting time. It's just kind of Byzantine.

In any event I would say that for at least this first part we are definitely grappling with what exactly is the problem, what exactly is the mandate, what exactly do you want from us or what is expected of us et cetera -- those things. That helps explain some of the current delay.

Mike O'Connor: Other constituencies? (Wendy), did you plan on writing something about respective of the (Alac) for example?

(Wendy Seltzer): Well (Alac) is not a constituency. Most people would liken (Alac) statement. I was planning to use the sole advantage of not being a constituency.

Mike O'Connor: So are you planning on writing something or...

(Wendy Seltzer): No.

Woman: It would be good though to try to get a feel for. And I'm not sure (Wendy) how best to do this or whether it can be done but kind of in a large sense. I mean I know they're following - you know, many at least are following this issue. And it would be great to find a way.

And I know we have others on the call representing - or, you know, who are participating on behalf of other organizations like (Bo) and others that also might be able to tap into some thinking there.

But, you know, given the breadth of this project, if you have any thoughts about that I'd really welcome them.

(Wendy Seltzer): Okay. I thought it would be easier to go to at large for comments if I could do that once we had definition.

Woman: Right, right. It may just be premature given that, you know, the organization. So just something to think about.

Mike O'Connor: You know, again, I think part of the problem, the process problem that we're up against here is that at least me, I was quite startled to discover how much difficulty we had simply defining fast flux.

And, you know, we may be on to evil money but when we had all this stuff out people, you know, we didn't have that definition.

And I would put forward the proposition that we don't really have a definition yet which is part of the reason why I'm so entranced with this sort of list of tasks or questions to answer in sequence that (Dave) came up is that we may be confusing the issue at this stage by trying to answer some of those very downstream questions like, you know, what should actually be done when we don't really know very well what it is that we're doing something about or how big the problem is or how it manifests itself or what its fingerprints are or, you know, there's this whole series of almost foundational pieces of seems to me needs to be done before we can really answer those questions. And that by answering them at this stage we're kind of pulling answers out of our hat.

Man: (Mike), I don't know that we need to answer those questions. I think maybe we should just try some solutions and the solutions might actually answer the definition things.

Mike O’Connor: Well, you know, part of the thing it seems to me that (Dave) laid out is almost a development work plan that says okay, let’s define what it is we’re trying to do. Then let’s build some algorithms just make sure that, you know, we can find the things that we’re trying to identify.

Then let’s build some code or find some code or if we if, you know, (Rod) mentioned earlier on the call that there’s some software in Australia that may embody, well it has to embody a definition of fast flux in order to be able to do what it purports to do which is identify fast flux host.

Maybe what we need to do is evaluate that software and see if we agree with its definition. I’m not necessarily saying that we have to start absolutely from scratch. But I’m really uncomfortable weighing in on what we ought to do when we are - when we don’t have these foundational pieces done yet.

Man: Well I think we should skip some of the foundations or get back to the foundations because if we get stuck there we’re never going to make progress.

Can anybody hear me?

Mike O’Connor: Yes, yes.

Man: (Mike), I do understand. These are all good questions.

Mike O’Connor: So how do we get these...

Man: So what do you then propose to do with all of the work data really, information opinions that have been expressed that people have spent, you know, untold hours documenting for the benefit of this group?

Mike O’Connor: Well I don’t know quite frankly. Because it’s not really in a form that’s possible to summarize. I mean, you know, you take any one of those spirited debates that we had, what they showed is that there’s disagreement, not agreement. And so how do you summarize disagreements except to say that there was disagreement? I mean we can certainly do that.

Man: You can’t document what the new opinions were or, you know, what the very - all of them - many opinions (are). That’s a bare minimum that we should be...

Mike O’Connor: Let’s presume that we do this. I don’t know exactly how but, you know, (Liz) and I can put our heads together on that later.

Would we recommend anything different than the list that (Dave) has published if we did that?

Man: You’re saying that basically your interpretation of the list or your summary of the list boils down to these open questions?

Mike O’Connor: Yes at this stage because, you know, I think that we just don’t have these answers. And, you know, I think, you know, for example if we just took the very first one, the definition - well let’s leave that one. We’ve beaten that one half to death. Let’s pick one that’s a little bit further down the list at random.

Identify data collectors, who can provide the data that we need in order to detect it well. We don't - in that earlier conversation on this call when we were, you know, when we were talking about the data that's coming into the workgroup we've given the data people a very difficult task in that we've not been able to define what data it is that we want them to collect because we haven't been able to define precisely what fast flux really means.

Man: And we've seen lots of different definitions of it. We haven't agreed on one uniform - one definition for everybody. But we've got definitions to work with. So we're talking about bad fast flux…

((Crosstalk))

Mike O'Connor: Right, bad bunnies. Now let's say that through magic we could get that definition nailed today, I still don't think that the working group, you know, unless we just completely blow away our schedule.

Let's presume a crystal clear definition for fast flux. Then the data people are going to have to go out and gather data. And it's going to take some time to do that. Without that data we've got no underpinning for a lot of the harm related, you know, issues, that whole conundrum because we don't know what's going on.

George Kirikos: (George) here. Can I join the queue?

Mike O'Connor: Sure, go ahead.

Let's see, hang on a minute (George). I haven't been paying attention to the queue. (Greg), you've got your hand up. Have you been patiently waiting or is that left over from long ago?

Greg Aaron: That's a leftover. All take that down.

Mike O'Connor: Sorry about that. Go ahead (George).

George Kirikos: One concern I have about the data is that I don't know if people are familiar with Baye's theorem. I posted it on the email list. But it's kind of very subtle but it talks about false positive rates and how it depends on the rate of something in a population. I posted it in the Evaluate Things Here window if you scroll up.

One concern I have about the data is that if we only study the criminal aspect, the sample data that you're working with isn't -is like biased. For example if you did a population - if the only data for example was a - on some matter it was the population of people at - in a certain prison, you never looked at for example the non-prison population.

Then if you become, if you only use the data on the prison population your test might seem very powerful. But then if you apply that test to the broader network of all humans, your tests starts to fail.

Mike O'Connor: Right.

George Kirikos: For example if you look at a prison population you might say oh, we've got, you know, lots of males. We've got people with two legs, you know, all things with two legs must, you know, must be criminals.

Then you didn't look at the total population and see that, you know, their characteristics there are, you know, don't allow you to necessarily determine the difference between what you're trying to test for.

Mike O'Connor: Right. I mean I'll use sort of a crass summary of where I think we're at. I think that what we've got here is a hammer looking for a nail. And I'm really uncomfortable proposing that hammer until we've got a better understanding of what it is that we're trying to construct.

(Mark), did you have your hand up?

Marc Perkel: Yes I have my hand up. Can you hear me?

Mike O'Connor: Yes.

Marc Perkel: Okay. One of the things I was thinking on this is, you know, is it a correlation between the fast flux networks and agent, the main? I would like to see, you know, are they using, you know, domains that are really newest as opposed to old domains?

Mike O'Connor: Hang on a minute (Mark). I think what I want to do is stay pretty focused on the process problem that we've got right now and save the content, if you will for another part of the discussion.

Marc Perkel: Okay.

Mike O'Connor: Good question but, you know, we're sort of at this juncture in what to do next. And I don't necessarily want to dive into the actual definition of things right now on the call.

Marc Perkel: Okay. But I think possibly we may be stuck on something that we don't need to be stuck on because we might not ever come up with a precise definition. But if we come up with solutions that don’t scare people then we might not -or other things might, you know, processes might lead us back to the definition think that we’re working on. I think we could get stuck forever on definitions and never get past that.

Mike O’Connor: Well, you know, you’ve made that argument before. And again, this gets me to the hammer looking for a nail kind of impression. I really don’t want to advance solutions without underpinning them. It just makes me extremely uncomfortable.

Marc Perkel: Well, okay. So perhaps I think we could agree that fast flux used for bank fraud is bad. Can we all agree on that?

Mike O’Connor: No I don’t - I really don’t want to get - I mean we’ve just got 1000 emails with variations of this conversation in them.

Marc Perkel: Right.

Mike O’Connor: And some people only want to call fast flux the bad stuff still. But (Dave) isn‘t that kind of right? That’s why I invented a new term. Bunny rabbit networks is good or bad.

Man: Right.

Mike O’Connor: And evil bunnies would be what some people call fast flux which will, you know, from now on we can call fast flux just the bad stuff if everybody agrees on that.

Man: Right.

Mike O'Connor: And there could be good bunnies which uses very similar - uses the identical technology say as fast flux but use it in a good way for free speech, you know, something else that hasn't been invented yet.

Man: I totally agree, whatever.

Man: Yes.

Mike O'Connor: So in the context of email for example, you have email being, you know, a neutral technology term, you know, illegal spam being equivalent to evil bunnies, the equivalent to what people are calling fast flux.

Man: Right.

Dave Piscitello: Well I've had my hand up a while. I'm going to jump in if I can.

Mike O'Connor: Oh I don't see it.

Dave Piscitello: It's - well it says actually it said I had the mic for like 5 minutes but I've been waiting. So I'm not certain why...

Mike O'Connor: The mic is when you're doing audio on these calls. Use the raise your hand button because the mike shows up sometimes just at random. Sorry about that. Go ahead (Dave).

Dave Piscitello: Actually, mine says raise hand. Anyway.

Mike O'Connor: Yes. There you go.

Dave Piscitello: I - my frustration here is that for weeks, you know, I've been trying to offer, you know, offer definitions. And we've gotten very close to definitions that allow us to call XNY as two distinct things. And we keep getting pulled back to using the term fast flux for both.

And I would be very happy if we simply didn't utter the word fast flux for about a week and just tried to identify the characteristics that were, you know, that will help us fill it out, a network that is doing criminal or malicious activity from one that is doing good.

I also believe that it's possible for us if we really want to get data that illustrate what a legitimate application of short TTLs and a legitimate application of volatile networking for the sake of high availability and resiliency is possible.

I, you know, if people believe that (Acami) is a model for that kind of network, I honestly believe we could get that kind of data. I honestly believe that we can characterize these two, you know, very distinctly without jeopardizing or sacrificing, you know, the - what we tend to call legitimate uses of, you know, these characteristics, some of these characteristics from the non legitimate uses.

But everyone keeps, you know, falling back and trying to defend their own perspective about, you know, about what is good and what is bad and don't throw the baby out with the bathwater.

And we're not going to get anywhere as long as people choose to just use the same nomenclature and believe that their particular need is at risk each time we talk about this. And that's all I'm going to say today.

Mike O’Connor: Oh I hate it when people do that. Oh well. I think that’s a really good point. I think that gets back to the need for a great definition of something, a great - you know, this - it seems to me that this has got to be built up on foundations.

And I’m stuck trying to figure out how to build that foundation. Again, that’s why I’m so attracted to this list of things to do rather than the very broad series of questions that I just don’t think we can answer those right now. But, you know that’s - I’m repeating myself too.

Other people got ideas? I’m looking at the queue. (Dave), you’ve still got your hand up. I’m presuming that at least for the moment you’re done. Anybody else want to try and get us off top dead center here?

My inclination as chair is to, I don’t know. I don’t know what to do. I’m stuck. I need some help people.

Go ahead (Dave).

Go ahead (Dave).

Dave Piscitello: I think that we need to go back and grab, you know, grab at least the definitions that Randy, I, (Joe) and (Mark) built over time and (Greg), and put that up as the definitive, you know, bad thing, the thing we want to stop.

And I think that it’s incumbent upon the people who claim that there are good things to come up with an equally, you know, useful list of good characteristics.

I tried to start that off today with an email that identified some of those characteristics. And I think we'll go nowhere until we have a very clear separation of, you know, of the characteristics that distinguish one from the other.

Once we have those clear characteristics I honestly believe that the kind of work that (Joe)'s put up and discussed in terms of illustrating that you can identify the bad thing and distinguish it very clearly with very low false positives is provable.

But if we doggedly try to say but they're a false positive, but they're a false positive with no real way of distinguishing the two, we're not going to go anywhere. You know, at some point people do have to make a concession that they're not putting something on the table to, you know, to corroborate their point, not say well we're only of looking at the bad things.

The fact of the matter is that the people who have been looking at the bad things have a lot of data. And the people who have not been looking at the bad things and claim that there are good things, you know, have not put data on the table.

I'm not saying it's not fair it's just that if that's how - if that's where you're committed and you believe in it than you ought to be coming up with the data.

Mike O'Connor: So, you know, this would argue in favor of the first, you know, I think it's perfectly fine for us to say look, here's a big long list of things that need - we found that the very first thing on the list, to improve our definition of fast flux is taking us much longer than we had thought.

We're happy to continue in that effort. But to answer some of the questions somewhat further down the list in our charter is very difficult without these underpinnings.

Our people - let's do a little poll on - I've just got an agree, disagree poll out there.

Can we agree to that or is there people - well it's - let's frame this very clearly, yes or no questions.

Can we step back from answering the whole series of questions at this stage or not? Yes or no?

Man: Sorry, what do you mean by step back?

Mike O'Connor: I guess what I'm saying is I am very - I am personally very uncomfortable trying to come up with answers to that series of questions in this workgroup given where we're at today.

And so I would prefer to say that list of questions can be answered and here's a process by which they could be answered and have that be our recommendation.

Man: Do we have to answer the questions in order?

Mike O'Connor: No. I don't think so. I don't think we can actually.

Man: You need to realize that some of these questions are really loaded with (absorptive) issues still.

Man: I concur with that. I really think that it may be useful to suggest more useful questions rather than to proceed with the questions we have.

How many false positives are we willing to manage? That’s not a decision for this group to make.

Mike O’Connor: Oh, no, no, no. Hang on a minute. I’m sorry. The questions that I’m talking about are the questions in our charter, not the questions that are in front of you today.

Man: No I know. But these are the substitute questions that you want us to direct our attention too.

Mike O’Connor: No, this is essentially a work plan for us. And it’s -let me phrase it this way. I think that what you see in front of you is a first draft that has not been hammered on in any way to get the consensus. So I’m perfectly willing to accept edits to these questions. And I’m sure (Dave) is too.

What I’m saying at this stage is that the charter is flawed and that the questions in the charter while they can be answered can’t be answered unless you follow some sort of process that looks something like the one that’s being proposed in the second set of questions, call it Question 2 for sake of clarity and discussion.

(Mark), unless - I’ll call on you but not if you’re going to hit me again with let’s look at solutions first. Go ahead.

Marc Perkel: I was just going to agree that the charter is flawed. And if the charter is flawed, what do we do then?

Mike O'Connor: Well I think that, you know, what I was beginning to type was to rewrite the charter for the working group as the very first thing to do.

And that in the process of doing that we could suggest - anyway, I'm not sure I can do - I can't - in a charter for a project often you'll find a good statement of what's the problem we're trying to solve and how should we try and solve that problem?

It seems to me that the list in Rev 0.1 form right now, but the Question 2 list is a pretty good start at a work plan on how two solve that problem.

But I think the problem needs to be, the charter needs to be rewritten because I think the way it's cast today it's impossible to answer those questions given what we know at this point.

Liz Gasster: (Mike), it's (Liz). I think that that's - if it comes to that again, I think some articulate description of why that's the case and what might be the alternative, you know, we still need this group's expertise to move on from that rather than just using that as a net result.

In other words then, you know, we've got to rewrite it and move on. I think we have the latitude here to do the right thing and not be constrained by what the council thought without the benefit of your expertise. In other words, they've kind of - they put something out there in order to solicit the benefit of this team's expertise.

I do not want to lose the fact that you all have brought this insight based on, you know, if it ends up being here is the data points. We have to have, you know, crafted in a way that is articulated and laid out some realistic next steps.

You can't - you know, this has the latitude to move forward the way it sees best and to comeback to the council even with an early report that crystallizes that and I'd be glad to help.

So I just don't want this group to be too constrained by specifically what it was told to do by a group of wonderful well intentioned people who were hoping you guys would help them figure it out.

Mike O'Connor: I agree with that very much.

Man: I agree too.

Mike O'Connor: (Mike)- just to give back to you (Michael) because (Mike), you're the one that was pushing pretty hard earlier in the call that we had to answer those questions.

(Mike Rodenbach): I think we can answer the questions. I have a difference of opinion in I think in how we could answer those questions now.

We may not be able two answer reach consensus to answer those questions but - in the time allotted. But we could outline the opinions that have been expressed so far and let the council decide what to do next.

It's also fine to say that (looked) at those questions, we've taken a lot of opinion and analysis. And we are going to make an effort to synthesize that. But we want to step back and look at this other set of questions which we think will help us reach consensus on a broader set of questions. I think the council would accept that.

Mike O'Connor: How, in our little poll, how do people feel about an approach like that where we do - we give our best shot?

Because I can, you know, I can do a summary. I'm just very uncomfortable treating it as the end all and be all.

(Mike Rodenbach): Absolutely. I hope we all are. And so like I said we haven't really made a good effort at synthesizing the opinions and coming to consensus.

Mike O'Connor: Yes and I would like some help on how to do that. (Eric), go ahead. You haven't spoken today.

A oh, maybe you weren't raising your hand. (Eric)?

Hang on (Mark). I just want to make sure that I saw (Eric)'s name pop up on the screen but I'm not hearing him.

Liz Gasster: And (Mike) I - it's (Liz). I want to ask you.

Mike O'Connor: Okay.

(Eric): I'm sorry about the delay. I had to mute and I'm finding my - the appropriate panel to Adobe which is why it showed me as coming up.

Mike O'Connor: Oh, okay. Sorry.

(Eric): Naturally I disagree with the council liaison who wants us to continue with the charter as stated. And I'm much more sympathetic to the position that we've articulated just a few moments how much we articulated on I think the first call where we grappled with the difficulty of the problem statements that we've had and that we've sent forth on the definition. That's it.

Mike O'Connor: Thanks.

Man: So (Mark) or (Mike)?

Mike O'Connor: Yes, go ahead.

Man: I have a proposed way forward.

Mike O'Connor: Cool. Go for it.

Man: What I propose is that we break down into two groups. One group defines what we believe to be the evil case and develop characteristics and indicators of, you know, of networks that we would feel, you know, we would have a very high confidence are, you know, are being used for evil purposes.

If the groups develops a similar set of indicators that would provide if run under test, a very high confidence of, you know, that we would be able to see them as benign and - or good or whatever we want to call them. Okay.

So now we'll have the two definitions. We can look at them very carefully and make certain that there's no overlap or as much as possible that there's no overlap. And then we can try to see if there is some way to actually develop an automation to do detection that results in low false positives for, yes, for each.

And I'm - you know, I'm more than happy to continue working, you know, to try to develop a definition of the, you know, the negative use of fast flux if somebody will step up and try to develop a definition of the positive use.

And I started that today and I really do think that if we can't draw a distinction between the two than we have very little hope of ever being able to do some automation. But I do believe that they're very easy to characterize and segregate.

Man: Agreed.

Mike O'Connor: (Eric)? Never mind. I don't know what I was thinking.

(Eric): I don't think I buzzed or beeped.

Mike O'Connor: Who's this?

(Eric): This is (Eric) since you've used my name in vain.

Mike O'Connor: Yes, I apologize. I'm getting a little overloaded on watching too many screens. (George) go ahead.

George Kirikos: I'm not sure that that necessarily is a good thing. because let's say for example you want to do a test to determine bad cars on the road or something like that or you want to get rid of all say, all trucks say. You're - those aren't necessarily going to be - well you want to necessarily have a definition for what all automobiles are too.

Like you might have say a good use might be cars. A bad use might be say trucks. But then that's a subset of all automobiles. You still might have you know, SUVs that are somewhere in between that you never looked at.

In other words you can have two non-overlapping sets that aren't the entire population. In a racial context for example you might have a test that determines, you know, whites and then blacks but then something comes along totally different, you know, a native person, an Asian that you never even thought about which doesn't overlap with either of those. But it's still a population of all people. So...

Mike O'Connor: So here's where I'm at. I'm liking the conversation that says let's get our definition in order. I think I would push back a little bit on (Dave)'s structuring but not the desire to get to a good definition.

And so what I'm hearing is support for the notion that we've got to get the definition hammered out and that if we can get that definition hammered out amongst ourselves in this working group, that may be as far as we can get. And we may not even be able to get that far.

If we can't get a definition, it seems to me almost irresponsible to make recommendations beyond that because we're building castles on sand.

So can I take it as agreed not - that we - there's no way especially given the fact that we're only ten minutes from the end of the call, there's no way that we can arrive at a definition today. But can we sort of boil together (Liz)'s point which is it's perfectly within our purview to go back to the council and say to them look, you framed the problem for us wrong. We want to reframe it...

Man: Agreed.

Mike O'Connor: ...as we need to and offer them a list of things that we want to do not unlike the list that's in front of you, the list two and then have at a very robust discussion about these definitions?

Let's do a poll on that. Go ahead and click whether I'm on the right track here or not.

Oh (Eric), in the notes box in the lower right corner if you scroll down to the section that's called Available Options, the series of steps, slash questions that (Dave) started and I've edited a little bit appears there. That's not been reviewed by this group at all. It's a start. And we'd have to build some consensus around that.

But that's what I'm talking about is that essentially we need to go back to the council and say look, there are a lot of things we agree on. One of the things that we agree on is that we need a really robust definition of what the problem is.

Another thing we need to agree on and - is how to identify these things. Another which - a contribution that I think (George) made which I think is a good one is a conversation about where those choke points might be to stop this thing. But we can't start that conversation until we have a definition of what it is that we want to try and stop.

And to leap ahead without that underpinning makes me nervous, really nervous.

I'm going to roll with that. Unless somebody hits me upside the head. (Mike), are you going to hit me upside the head if I do something like that?

I'm taking that as either no I won't hit you upside the head or he's not on the call anymore.

(Mike Rodenbach): Sorry I'm on the call. And I was on mute and I was talking to myself for a moment.

Mike O'Connor: Ah, sorry. It was probably very eloquent. Sorry to have missed it.

(Mike Rodenbach): No one will ever know.

Mike O'Connor: No one will know.

(Mike) So what I think I was trying to say was that you know, I'm okay with the approach (Mike), but we do need to make the effort to answer the question at some point. I consider this a step in that effort.

Mike O'Connor: Oh think in some infinite amount of time, maybe a year, certainly those questions could be answered as a result of a process like the one that (Dave) has laid out here and that I've edited and that we could beat on really hard.

But I don't think we can answer those questions in the 90 day window of this working group. And I think we need to give (GNSO) a heads up about that and then give them a positive proposal as to what we would like to do and...

Man: Definitely agree.

Mike O'Connor: ...maybe even estimates on timeframes as to when that might happen.

Man: So I think that yesterday I told the council that we were well on track.

Mike O'Connor: Well, did you ask your chair before you told them that?

Man: I saw your status update today. It makes it look like we're all on track.

Mike O'Connor: Yes I know. We'll I was lying. You (fucked up). You trusted me. Sorry about that.

Man: I mean...

Mike O'Connor: And, you know, I do feel that if we could - if you scroll around in this little report that's down in the lower right corner, I think we could issue a report like that. Essentially that's, you know, I just don't - I don't think that this report can answer those questions. This report is essentially answering a slightly different question which is what...

Man: What I would suggest we do the next week or ten days then is come up with a brief narrative as to why we think we can't answer consuls questions without answering these other questions first.

Mike O'Connor: I can do that.

Man: And I can get it on the agenda for our September 4 meeting and likely get it ratified.

Mike O'Connor: That would be good.

Well I think that what that would be in my consulting days I used to call this the big whoa conversation where we would go into the client and say whoa, wait a minute.

Man: Yes.

Mike O'Connor: We're - we need to have a stop, take a deep breath, recast the problem conversation. We're happy to continue but the path that we're on right now is going to lead to an unsatisfactory result. And I'm happy to do a first draft of that.

Man: Yes, I think it's something that, you know, everyone should have a chance to comment on.

Mike O'Connor: Yes, yes, for sure. And we- you know, we could either shoot for finishing it up on the lists or we could finish it up at that meeting next week. We'll see how it goes on the list. But you know, I'll take a crack at a first draft on that.

Man: And like what (Liz) was saying, you know, the most important thing is we really - one of the groups that have been active, engaged and we've used the material that we've got so far. So...

Mike O'Connor: Oh well, you know, I think that the conclusion that we're presenting rests on pretty solid foundation. I just don't think that we've got it done yet.

We're 2 minutes from the end of the call people. I'm going to take that, you know, say that this is probably the last chance to comment on this proposed direction. Let me restate it.

I'll go through and write up. I'm not even going to restate it. I'm going to listen to the MP3 stuff because I think that we've already described it pretty well.

Are there folks who want to weigh in on the other side at this point? If not...

Man: I just want to disagree with the idea that we should stop everything else until this is done.

Mike O'Connor: Well...

Man: So for the order part of it, you know, and let us precede asynchronously, I'm for it.

Mike O'Connor: I am not at all opposed to carrying on with other efforts especially aimed at solutions. I thought (Joe)'s little gizmo was - (Joe)'s gizmo actually triggered a lot of questions in my mind. So I'm happy to let that continue.

But off list, quite frankly, I am bewildered by the 1000 emails in my inbox and can't handle any more on that.

So if folks want to continue working on solution designs or conversations like that, that's fine. But, you know, recruit amongst yourselves and then carry conversation off list.

Other thoughts? I'm not even going to take the mandatory how's (Mikey) doing. I don't want to dough. I'll take that up next week.

I appreciate by the way, all of the very helpful off list replies to my - what I'm calling my sad note earlier this week. It helped a lot.

That's it folks. It's a 11:30 and I'm going to declare us adjourned.

Woman: Thanks (Mike).

Woman: Thanks (Mike).

Woman: Thanks (Mike).

Woman: Thanks.

END