Fast Flux PDP WG Teleconference

TRANSCRIPTION

Friday 1 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 1 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-20080801.mp3
http://gnso.icann.org/calendar/#aug

Present:
CBUC
Mike 0'Connor - WG Chair CBUC
Mike Rodenbaugh - CBUC - Council liaison
Zbynek Loebl ISPCPC
Registry Constituency
Adam Palmer - PIR (registry constituency lead)
Greg Aaron - Afilias
Rodney Joffee - NeuStar
NCUC
Christian Curtis - NCUC
Registrar constituency
Eric Brunner - Williams - CORE
James Bladel - Godaddy
Kal Feher - MelbourneIT
Eric Brunner-Williams - CORE
Ihab Shraim – MarkMonitor

Wendy Seltzer - ALAC liaison ICANN Board
Beau Brendler - ALAC
Observers - (no constituency affiliation)
Dave Piscitello - SSAC Fellow
Marc Perkel
Rod Rasmussen - Internet Identity APWG
Randy Vaughn
Joe St Sauver
Staff:
Liz Gasster
Glen de Saint Gery

Absent - apologies:
Marika Konings - staff
Paul Diaz - Networksolutions

Coordinator: The conference is now recording. You can go ahead.

Mike O'Connor: Thanks very much.

Woman: Okay, (Mike), I'll start. Mike O'Connor. Staff, we have (Liz Gasster) and (Marika Konings can't be on the call unfortunately, (Christian Curtis) (unintelligible), (Adam Palmer), (Kal Feher), (Mike Rodenbach), (Rodney Joffe), (Wendy Seltzer), (JamesBladel (Greg Aaron), (DavePiscitello , Marc Perkel and (Rod Rasmussen).

Have I missed anybody?

Mike O'Connor: Yeah, you missed Glen. And Glen is on the call.

Okay, here's the agenda folks. I think we've got a pretty comfortable conversation to have today, but I think it'll probably take the whole two hours and if anybody wants to add to it we'll try and stick it at the end. Can everybody hear me okay? When I was listening to the recording of the call last week I thought I was kind of quiet. People can hear okay, I'll take that as a yes.

Man: Yep.

Man: Very good at this point.

Man: (Unintelligible).

Mike O'Connor: We'll take a quick look at the stuff we did last week and get some updates on those issues, then I've got some tasty discussion topics for us that I hope will evoke lots of conversation, and we'll then wrap up by looking into next week.

And with that I'm going to switch to the status report which looks like that. And in the status report this week I'm happy to report that there's nothing to care about, we're on schedule, we seem to be making good progress, we've got scope under control, so this is the kind of status report we want to see.

We did a lot of stuff last week people. We've. I think had, a pretty energetic and productive conversation about both the definition that we want to use for Fast Flux and the scope which sort of got folded into the same one. We're going to go through that a little bit later but I just want to give us a pat on the back collectively for what I think was pretty good work.

Let's see. I'm getting a lot of (unintelligible) here. Everybody else hearing me three times too?

Man: Yeah, I've got an echo.

Man: Yes.

Mike O'Connor: I don't know if it's the speakerphone is not muted.

((Crosstalk))

Woman: I (unintelligible).

Mike O'Connor: Okay. Yikes. Well, anyway I'll carry on and listen to myself, see if we can get through this. We kicked off several discussions which I think we'll probably carry on this week and those fell into sort of a benefits area and then proposed solutions we kicked off a bit. And I'll save

plans for next week for later but we are getting to the end of the first informal input constituency round in at least in the BC we're starting to get some results to that. And I might have some commentary about that template later, we'll see.

Anyway that's the status, your (unintelligible) is all good, we're fine no issues, my favorite kind of status report. So now I want to move onto the next part which is to take a look at some of the actions that we had outstanding last week and I think I'll kick it off with just a conversation to touch base with the data people, (Dave), (Greg), (Rod), (Rodney), how's that going? Are we making progress there?

Rodney Joffe: So on my stuff, had some logistical problems in that we have so many domains it turns out and a few of these that are rate limiting queries that it sort of slowed down us getting the first round of data which is to identify - just so you know there's four classes that we broke this down into domains that the registry showed that we would delegate it as well as someone else being delegated.

So ultra (unintelligible) plus perhaps the customers and so they're the domain holders themselves, domains that we showed that we were delegated in the registry. In our system there were additional name servers that where actually configured which are the ones that we think are the most interesting. And then what we've done is we've (unintelligible)back onto see where the differences and what we're now doing is actually doing the - I think we're finished being able to give all that data on the registries later today.

And so it looks like it won't be until Monday morning before I can actually give you the detail - all the data that we were looking at last

week, but I will have it by Monday morning assuming that's not too late.

Mike O'Connor: Oh, it's fine. You know, I'm pretty relaxed on how we're doing in terms of making progress here. I think that's going to be more than fine. Yeah. Again, hats off to you and your folks for undertaking that project. I think it's going to be really helpful to see the results, so thanks for that update. That was (Rodney) by the way.

Others, (Dave), (Greg), (Rod), how's the stuff going on your projects?

(Rod Rasmussen): This is (Rod), not to be confused with (Rodney).

Mike O'Connor: Yeah, thank you. We had some off list conversation about that.

(Rod Rasmussen): Don't worry. We've gotten several people who are volunteering to send us data we haven't seen a lot of it yet, but a couple different security companies and researchers are trying to put together some stats to contribute to the project.

You know, gotten connected in, in the last day here or two, a project that's being run out of the University of Milan that should have thought of - a lot of you may have heard about this before - it's called the Fluxor Project and they're actually tracking, looks like about a 120,000 domain name getters on their definition of Fast Flux, including several benign ones, as they call them, so I think you get data from both sides of the equation here.

Mike O'Connor: Good.

(Rod Rasmussen): They've got a very cool Web site with very cool graphics on it, but they don't have - on that Web site they don't have the ability to actually take a look at kind of the under (unintelligible), so we've got some outreach going onto them right now. I don't know if anybody else in the group - how many have a direct connection to them?

It's the University of Milan Flexor Project. I don't know if (Joe) may have some connection there, but I've been introduced to some contacts at Iron Port who work with them. So I'm hoping to get some data out of them next week because they have an active project tracking all this stuff, at least the stuff that they're seeing and it looks very exciting.

Mike O'Connor: That's terrific. If you need any help from me as the chair on an email don't be shy, I'm happy to write...

(Rod Rasmussen): No, I don't - believe me I wouldn't - I won't be. I just got my, my formal introduction letter just came in the - my email this morning due to the person running (unintelligible) from my - I guess my trusted introducer as we say in the business.

Mike O'Connor: Yeah, terrific.

(Rod Rasmussen): So hopefully we'll be able to get under his web in some of the data they got there and bring that into the discussion here.

(Liz Gastor): (Rod), this is (Liz). If you happen to need help with either interpretation or translation you should let Glen or I know as well.

(Rod Rasmussen): Okay. Yeah and I - from the looks of it the person on this is an English speaker but, yeah if we have an Italian translation issue I'll definitely check for that.

(Liz Gastor): Now, I'm not volunteering personally, I'll just help...

(Rod Rasmussen): Right. I realize that.

Mike O'Connor: Cool. Okay. (Dave), (Greg), anything from your efforts?

Dave Piscitello: Well, my efforts are in parallel with (Greg)'s and I have, you know, I'm in the same situation that he is. I've had people offer me data, in particular, this week I got someone from Australia who, you know, sent out some very interesting data and he asked me what out of his 700 megabytes of data I might want and I checked him off with a number of, you know, a number of ways to look at the data and he said he'd get back to me.

But most of these people have full-time jobs and, you know, offering data is a nice thing but, you know, as (Rodney) attests, once you get into trying to, you know, distill data down to a specific, you know, a specific request it takes some time (unintelligible)and the like and that doesn't happen overnight. So.

Mike O'Connor: Yeah.

(Liz Gastor): So (Dave) it's (Liz), if you need any help with interpretation or translation there too?

Dave Piscitello: Well, I think the vast majority speaks pretty good English.

(Liz Gastor): Okay.

Man: (Mark) can perhaps help there as well if you like?

Mike O'Connor: I was just going to say we have Australians in our group already.

Dave Piscitello: Yeah, we've got plenty of Australians around the place and I can always ask (Paul).

Mike O'Connor: Okay. Great.

(Rod Rasmussen): (Dave), is that (unintelligible) or is that somebody else?

Dave Piscitello: Speaking of data (Rod), thank you very much for the data you did send me. I'm, you know, I'm going to start to part through that because I like to take advantage of it and I want to go see the (unintelligible).

(Rod Rasmussen): Oh, is that (Ausfort) or somebody else in Australia?

Dave Piscitello: You know what, I don't have it right in front of me but I'll let you know. Yeah.

(Rod Rasmussen): Okay, because I've been reaching out to (Ausfort) too so - and they may have some data. Okay. Thank you.

Mike O'Connor: I don't need - okay. All right. Anything else on data? It sounds like data is in good shape, I like the sound of all this.

Legitimate user is next, (Wendy), (Greg), (Mike)? I got to the bottom of my barrel of legitimate users so I've got nothing to report beyond what I did last week. Anybody else around?

(Greg Aaron): Yeah, this is (Greg). I missed a lot of last week's meeting, so I don't know which examples you had discussed. Could you recap briefly for me?

Mike O'Connor: Briefly, I got to Compton West Publishing DTO and Chief Information Security Officer and sort of put the outlines of the question to them thusly, you know, we're looking at Fast Flux as an issue.

One of the fastest of that is low TTLs on both hosts and DNS servers, what sorts of TTLs do you use in your environment and is there a difference between the way you do it on hosts and DNS servers and what would be the impact to you if we were to use (crocarian) logic some sort of token permissioning thing to perhaps control low TTLs, especially on the DNS host's side - the DNS side not the host side.

And the word I got back from both folks at Thompson Reuters and the folks at A Startup, that actually does a lot more traffic than Reuters does, was that they use pretty low TTLs, especially on their host side. The Reuters standard TTL is 30 seconds and, you know, as (Rodney) said in his part of the conversation yesterday there's some people who set their TTL to zero.

So there are legitimate users that use really low TTLs. They were somewhat less than totally ecstatic about the idea of the (crocarian) logic primarily because of the concern about introducing another point of failure and as you might expect folks who run really big data centers

get grouchy about that. But they weren't panicky grouchy, they were just...

(Greg Aaron): Okay. Yeah, I think the issue of low TTLs, I mean, I think that's going to be definitively settled. The RFCs allow many, many legitimate uses. I think, then that in another way is there anybody out there that makes rapid or repeated changes to their names - to their resource records?

((Crosstalk))

Mike O'Connor: On NetWare everybody sort of agreed that that was much more unusual.

(Greg Aaron): Yeah. What I'm going to do is I'm going to summarize that off list conversation that a few of us had looking at a particular example because we weren't sure what to make of it. I'm going to summarize that thread and send it out to the group.

Because I don't think we're still not able to make heads or tails of it in a lot of ways and it's probably not the best example but it's of interest and fair enough to throw it out there for examination. I won't go into the details because I'll post just a - what we know and what we don't for the group.

But there's a - we found an example of a service and we're not - it looks like it uses the technique of rotating IPs and so forth but we're not sure whether it's a service that is criminal or not and that's what - there's a lot of complicated questions around this kind of thing.

I think what we're really talking about is what's going on out there in the wild on the internet? And the answer is, we don't know or we don't have a good feel for it. And so any - we have to figure out, you know, if the particular solution or - was implemented what might be the results. And right now I don't' know the answers. So let me take it upon myself to summarize that and send it out.

Mike O'Connor: Terrific. You will find yourself immortalized in the action items for next week.

Okay. Let's see, we've covered (Rodney)'s thing, and I then I just want to briefly drop us in on a Fast Flux definitions for those of you who weren't right on top of the only you know - last week was a pretty moderate week, I think it was only 200 or 300 emails so, I'm a little concerned that we're going to easily break the 1000 email barrier but I'm concerned that we may flatten out, we may not get to 2000 as we were current (unintelligible).

This is where we wound up at that end of the definitions discussion. And I'm not sure I want to actually go through this in detail now on the call because we did spend an awful lot of time on the email side of the house going through this, but this is starting to edge into preliminary final draft stage in my mind.

So this would be a good time for those of you who haven't followed every single email to sort of check back in and see how we're doing because I think we made a lot of very positive useful progress last week in email on this and I think it helped in a lot of ways. It helps with the data discussion; it helps with the solutions discussion.

So, you know, I think just leave it at that, sort of an attaboy for us having had the progress we did, but it's time to sort of zero in on this one and make sure that we've got it right.

And I'm not even going to encourage discussion - I really wanted to start three new discussions. I do love the fact that these calls are recorded because I don't have to take notes but I am starting to edging around in my own mind, at least, as far as writing as a first draft of the final report or at least the interim report, and I may try to get that draft out for next week' call.

Even though it's clearly got lots and lots of stuff still coming in, I think it's getting to the point where we can start to actually edit a draft. And the first thing that I wanted to try out on the group as I was sort of writing my draft was a headline because I think it's useful to come up with, you know, a kind of broad statement of what we want ourselves to be remembered for.

And the headline I came up with was 'ICANN helps reduce Fast Flux Hosting' as sort of a summary of - a desired outcome of what we're trying to do here. And I put this up in my standard sort of village idiot way. I have no editorial pride; I just want to kick off a discussion that fits us to a sense as a group of what we want to be remembered for.

And again, let's see can I do this? Let's use the raise handing thing for the queue like we've been doing. For those of you who are new to the Adobe Connect gizmo, if you want to raise your hand all you have to do is click on your name - actually I'll - I bet what happens is this - is this recursive?

I don't know if this is - I bet this is recursive. But let's say that I wanted to raise my hand, I could click on my little name and then I could - what can I do, no I don't want to do that. Somebody remind me how to raise your hand.

Man: It is actually below the text - the IM facility, once you click on your name just below that there's a little - so if you take your curser below the IM window.

Mike O'Connor: Oh, yes. Yes, yes.

Man: Just a little bit lower I think. Your (unintelligible) is slightly different to mine, I'm on a Mac, but I believe it will be below...

Mike O'Connor: Ah, you're right, there we go its - way at the bottom of your screen is a little button that you can use to raise your hand and (unintelligible).

Anyway, what that does is it gives us a queue and it makes it really easy for me to see who wants to talk, so if you want to get in the queue just click the raise hand button and I'll see it and off we'll go.

Right, so there you go. How is that headline? 'ICANN helps reduce Fast Flux Hosting', have at it people. Don't all raise your hands at once? Does that mean it's really good or does that mean it so bad that people are shocked and can't figure out how to even approach the problem? Go ahead, (Mark).

Marc Perkel: I'm not sure that's the best title for it because we're not stopping - Fast Flux Hosting is just a method - we're fighting fraud and abuse so I

would think that, you know, maybe something along those lines might be better.

Mike O'Connor: Okay, others? I'm not going to even take notes. I love the fact that the call is recorded. What I'll do is I'll just sort of synthesize this conversation as we go and - so, I mean, one way to write that headline would be to say 'ICANN helps reduce Fraud, Phishing, fill in the blank, by zeroing in on Fast Flux Hosting' something like that. Does that work better for folks?

It's either really good or really bad. I'm not concerned at all if it's really good, I'm only concerned if it's really bad. I could do a poll. Do you want to do a poll? I can do one.

Marc Perkel: It's not really bad, you know, I mean it's - that's reasonable to me.

Mike O'Connor: Let's see if I do - if I push this button what happens? Oh, yes this is our anchovy pizza poll. Hang on a minute. How is the headline, question mark (unintelligible), good, bad. All right got it open, you should be able to vote. You should be seeing results; I'm hoping you see results. I'm not counting any votes.

(Christian), go ahead.

(Christian Curtis): Sorry, I was disconnected briefly. Could you repeat what the headline is?

Mike O'Connor: The headline is 'ICANN' - let's see, I'll take (Mark)'s friendly amendment - ICANN helps reduce Fraud and Phishing, fill in the blank, on the net by zeroing in on the Fast Flux Hosting problem', something

like that. The original headline was 'ICANN helps reduce Fast Flux Hosting.' (Mark) wanted to broaden our attention to saying well we're really trying to reduce fraud, phishing, etc. and so I, you know, in a fairly lame way inserted that into the headline.

So we got a sort of - can people see the results? Can you see the 2/3, 1/3 results?

Man: Yes.

Mike O'Connor: Okay. For those of you who are in the 33% that are thinking this isn't so great, chime in at this point and help us make it better. (James), go ahead.

(James Ladera): Thanks, (Mike). I just had a couple of ideas or suggestions to throw out to the group. One would be to replace the word 'help' with something like a more action oriented verb like investigates or studies or examine.

And I think that reduction or elimination kind of gets ahead of ourselves by pre-supposing what the outcome of all this effort will be, so maybe something that just focuses on the examination or the investigation work I would be more comfortable with. But those are just thoughts at this point.

Mike O'Connor: That's good. Others? Switch back to -- go ahead (Greg).

(Greg Aaron): I think the ambit of our working group is to examine possible policy solutions, but I think we're getting ahead of ourselves by saying we're coming up with solutions.

Mike O'Connor: Okay. So ICANN addresses, investigates, technical and policy - I'm not going to do this, this is a bad idea - I'm not going to edit at the same time I'm going to just talk (unintelligible) computers out there. Thanks, (Greg). Others?

I'll just take all of this and mesh it together into another headline. We'll have lots of chances to beat this headline up as we go because, you know, it's sort of the kick-off, but this is very helpful.

Okay. I'm going to close the poll and go back to sharing. Anybody got anything else to say about the headline or did the comments sort of cover people's concerns? Last chance.

Okay. I'm going to move on now to the impact of Fast Flux and I want to throw an idea out to the group and see if this understanding that I've come to is on the right track. We had a lot of discussion about the impact of Fast Flux and one of the things that emerged for me is that the impact of Fast Flux is difficult to separate from the impact of all of the techniques that Fast Flux assists in, like Phishing, SPAM, Malware, etc.

So most of the impacts that we described are impacts of those techniques that Fast Flux is sort of part of the toolkit of, it's an enabler of. And that was really hard for us to - and I maybe I took us down a blind alley by saying "Well yeah but, what can we attribute - what can we lay only at the door of Fast Flux?"

And as I've reread those threads and cogitated about it seems to me that another approach to this is to say that it - essentially, to just say what I just said which is, "Fast Flux is an enabler to a bunch of bad

things. They have a bunch of impacts on a lot of people. We're going to restate those at a very broad level but not try to arrive at the definitive answer because that issue has been explored by - in much more depth by many others.

And that's - what we're interested in is the fact that Fast Flux is a technique that helps people do that and try and figure out the impact on that broader problem that could be laid to the - at the doorstep of getting rid of Fast Flux in a sort of hypothetical way.

So in other words, not try and attribute impact directly to Fast Flux, but rather to just say Fast Flux is an enabler that allows a whole bunch of these things to happen or assist people in doing those things. And it's our expert wild guess that we can reduce that impact, probably in a non-quantifiable way, by reducing the availability of that tool to the bad guy and I 'm trying to say this in a succinct way and being Irish that's really difficult.

But does that A, is that fairly clear and B, is that a reasonable summary of our position at this stage of the game?

Go ahead. Again, don't all raise your hands at once.

(Rod Rasmussen): (Mike), this is (Rod) I actually do have my hand literally raised, but...

Mike O'Connor: Oh, you do. Cool.

(Rod Rasmussen): One, I think that - and I think this touched on something (Eric) brought up on the list - like the week before last but, you know, we've

got all these different harms out there why do we care about Fast Flux more than - differently than anything else?

Mike O'Connor: Hang on a minute, (Rod). I'm going to encourage us all to mute - somebody's got either a speakerphone or something going on with a lot of background noise that's making (Rod) almost impossible for me to hear. Thanks, folks. Go ahead, (Rod).

(Rod Rasmussen): Okay. I think this addresses something that (Eric) brought up on the list is why are we looking at - why do we care about Fast Flux differently than all the other ways that people put out these fraudulent (unintelligible), whatever adjective you want to use Web sites.

And, you know, that's - it's a very legitimate question and because there are - all of the behaviors we're talking about here as far as the types of harm that are coming to individuals and all the, you know, millions, billions, trillions, whatever amount of dollars of damage it's causing, they can all be done using different techniques.

I think that one of the things we need to quantify and I think we can quantify this, I think there is some data on this is why is Fast Flux so much more effective and how much more effective is it than a standard type of exploit? The (unintelligible) used...

((Crosstalk))

Mike O'Connor: Really?

(Rod Rasmussen): You know, as far as...

Mike O'Connor: You think you can quantify that?

(Rod Rasmussen): Well, we certainly have examples of that.

Mike O'Connor: Wow.

(Rod Rasmussen): There's the Cambridge study on phishing for example, look at Fast Flux and (unintelligible) lifetimes versus standard hack servers or other, you know, types of phishing sites and found that the lifetimes were, you know, five times longer or so.

((Crosstalk))

Mike O'Connor: Oh, that's...

(Rod Rasmussen): Yeah.

Mike O'Connor: ...great.

(Rod Rasmussen): Yeah and...

((Crosstalk))

Mike O'Connor: I mean it's not (unintelligible) world, but it's a great...

(Rod Rasmussen): Well, yeah. I mean and that's why this is - that's why a lot of people in the security community have been raising this issue. If it was just as effective as any other technique I don't think we'd be putting quite as much emphasis on it but because of the way the bad guys are using

this system and it's leading to much longer times for these sites to be alive it leads to much more harm.

And I know we've got some data from at least a couple of our financial customers who look at exactly that, right? What is the impact of a site being up, for say, five hours versus five days? There's actually hard dollars that can be extrapolated from that.

Mike O'Connor: Sure, absolutely.

(Rod Rasmussen): So I've got that kind of information can certainly bring in the Cambridge information, but I think that that should be part of the discussion here as to, you know, what we're trying to do here and why, you know, why we're attacking Fast Flux and trying to do something about it.

It's not just that it enables this stuff, it's that it's better at enabling this stuff than a lot of the other methods that are out there and as a result criminals are using it in what appears to be larger and larger amounts.

Mike O'Connor: Right. I think that's a nugget that whole piece of the conversation. Do other people want to dive in at this point? Oh, I'm sorry I'm not paying attention somebody I think had their hand up and it disappeared off my screen, somebody go ahead and dive in.

Marc Perkel: This is (Mark) and I'm going to agree with what was just said. And also I'd like to include that usually Fast Flux by itself isn't a method of fraud. Usually Fast Flux is combined with spam for instance that points to the Fast Flux domain, so I think that some of the other techniques, you

know, need to be sort of looked at in that how are they used with Fast Flux.

You know, for example, spam that points to Fast Flux. So, you know, it's first the victim gets the spam saying that the (unintelligible) has been limited, click here to put in your username and password to unlock it and then that points to a domain that's Fast Flux, so I think we should have sort of like a broader look at about how Fast Flux is used in combination with other types of broad techniques.

Mike O'Connor: I think that's an interesting idea. I don't want to go into an exploration of all of spam because that gets too big and it would slow us down too much but the idea of how Fast Flux amplifies some of those other techniques and again data to support it would be...

Marc Perkel: Or how they interconnect because you see if you have Fast Flux being driven by spam if you can stop the spam then the Fast Flux becomes less effective and if you know the domain that's Fast Fluxing you can make a decision as part of, you know, information of other things to stop the spam that points to the Fast Fluxing domain.

Mike O'Connor: Yeah. Yeah. I get that. Others, anybody else want to dive in on this? I mean I'm not hearing anybody saying that I was wrong in that first rant. I take both of these as sort of course corrections but rather than try and - and I think part of the reason I want to have this discussion - and (Mike Rodenbach) I think you're on the call I hope - this is partly because I kind of want to change the framing questions.

When we talk about all these different kinds of folks who are harmed, it gets us distracted in a way. And what I'd rather do is sort of take all

those harm questions and sort of lump them together and say look the whole community, all these different stakeholders are harmed in different ways by the same thing.

And rather than try and put them in silos essentially sidestep the whole issue by saying what I'm lobbying for here which is Fast Flux can't be pinned with specific harms, it's the fact that it enables - and to (Rod)'s point - makes more effective harms that are already defined.

I'm hearing the silence of, yeah it's close enough, go ahead (Mike). So this is your last chance to give me a course correction; if not, I'll sort of carry forward that approach.

Thanks (Rod) and (Mark) for the clarification.

(Eric): This is (Eric).

Mike O'Connor: Oh, go ahead (Eric).

(Eric): (Unintelligible) that I posted earlier a disagreement with that approaching. Thank you.

Mike O'Connor: Got it. You want to come back with a counterpoint or do you want to just be on record as disagreeing?

(Eric): As there appears there are a lot of problems with the phones I think just being on record is sufficient; however, it's all in the notes that I sent on benefits and a previous note on harms.

Mike O'Connor: Okay. Got it. So is it - are other people having a hard time hearing the call or is it a problem with (Eric)'s connection?

Man: I'm having (unintelligible) as (Eric).

Mike O'Connor: Yeah. I think - (Eric) I think your connection may be at fault here. You were breaking up a bit when you were talking, so sorry to hear that it's not going so well for you.

Okay. Carrying on with my village idiot style of conversation, one of the conversations that I kicked off yesterday, I sort of want to again take some free form time to kick around in this group and this is the notion of essentially turning the harm discussion on its head and saying, "What are the benefits of doing something about Fast Flux? Who benefits? How do they benefit?"

What I did just for fun because (Joe) pushed along some really neat huge numbers which allow for silly math -- and I love silly math -- is I did some silly math on the net or on the email list where I took all of (Joe)'s numbers, which are by no means I'm sure all of the harm that's really associated with all these techniques, but it added up to a $500 billion a year pile, which is enough.

And I did sort of effectiveness math and got us down to the point where you could say if we could reduce that harm by .25%, we'd be saving something on the order of $600,000 an hour because, you know, that's the beauty of large numbers like that is you can get giant numbers back.

And I - (Dave) correctly came right back and said, “Be careful what you promise.” And I came back on that and said, “That this is really more of a statement of aspiration than it is a promise.” In that I think its good for us to think about this would help people. What’s in it for them? What’s in it for the Registries? What’s in it for the Registrars? If we could do something constructive here, how could people get motivated to get up in the morning and help move this cause forward?

And so I’ve thrown out sort of four topic areas that I’d just like to spend maybe, I don’t know, five minutes on each just brainstorming. Again, this will all come back to you for editing and we don’t have to worry about outlandish notions at this point, but just to kick it off how could - you know, if you think about in the true Deming Baldrich Award winning sense of quality, which has lots and lots of richness for those of you who’ve spent time in that community. I don’t want to go through the whole definition, but there’s a lot in the quality jar.

How could doing something about Fast Flux improve the quality of either the experience of a customer or the delivery for a producer of services? And that could range from, you know, if you think about quality as a way of reducing errors, you know, how could this reduce errors for people? How could this in any way improve the quality of the experience of the internet for its users and its providers?

Mike Rodenbaugh: It’s Mike Rodenbaugh. I jumped in on that I think.

Mike O’Connor: Go for it.

Mike Rodenbaugh: Isn't it by the necessity if you ended all of the criminal and malicious Fast Flux activity on the various networks, doesn't that by necessity mean that everybody else would have faster and better resources.

Mike O'Connor: Yeah, so you would remove, you know, and that would be an improvement of risk - you know, the quality of the service.

Mike Rodenbaugh: And also it takes away a potential threat to (unintelligible) a Registrar or Registry, one of these (unintelligible) out of hand.

Mike O'Connor: Right. Which would, you know, mean that they could spend less time on that kind of stuff and devote those resources to improving their products in other ways? Since I would presume that right now dealing with all this stuff consumes a fair proportion of not just Registry-Registrar but you know business, access provider and customer resources.

That's partly a cost or resource avoidance, but another way to frame that is those resources can - that you use to spend on those things can now be applied to making your product better, getting more customers, generating more revenue.

You know one of the problems with all of this stuff is that all - almost all of this activity is entirely non-value added to the enterprise that can be removed. Nobody is in business to deliver any of these things, they're doing it because they need it in order to provide their customers a reasonable experience or to keep criminals away from them. But they're, you know, there isn't much value add-in in fighting Malware, it's just a necessity.

Now, it seems to me that another facet to this - and it came up on the email list - is that there's a reputation component that touches almost every stakeholder. You know, the harm is loss of reputation; the benefit, it seems to me is that if a Registrar-Registry business customer whatever has this issue addressed then their reputation isn't necessarily higher and that might be a selling point.

It might be that a, you know, pick somebody in the business community - let's say a bank figures out a way to deliver their services over the net that is absolutely secure against attack -- this is all hypothetical -- and let's say that they are the only bank that has that. Well, that might be a competitive advantage for them in getting customers. The same it seems to me might go for Registries or Registrars.

If a Registry is perceived to be safer or even better yet demonstrably safer, it would seem to me that that might be a competitive advantage for that Registry and that that might in turn motivate others to compete with them to bring themselves up to that level of capability.

You know, one of the things that wound up costing and essentially justifying the whole security program in Minnsque, the state college and university system here in Minnesota that I ran for a while was the discovery that we could teach classes on security to students because security is really a hot area right now, and we could - by getting really good at security - pipe some of the knowledge that we had on the security team side out into the curriculum and bring in more students.

And in fact we wound up making a profit on the security cost center last year because we brought in more students than the cost of running

the center. So that's the kind of thing I'm hunting for right now, is sort of the opposite side of harm. It's the harm discussion, but it's inverted. Anybody else got any ideas of really good things that would happen, not just quality but, you know, let's open it up to all the other stuff.

Response time is one that it strikes me that is at the core of a lot of our discussion right now. You know, (Rod)'s point that a five-hour site is much worse than a five-day site and the fact that the bad guys are getting their response time...

(Rod Rasmussen): Other way around.

Mike O'Connor: What's - well, a five-day site is worse right? Whatever...

(Rod Rasmussen): Yeah.

Mike O'Connor: ...I said. Yeah, sorry about that. Old guys do that. Thank you. It seems to me that the bad guys have the response time argument figured out. They've - they're getting much better at responding and that to the extent that we can get better at responding that's a good thing.

I think that that's a justification, especially for a lot of the instrumentation information base kind of proposals that we've been floating, in that it reduces the response time of the good guys and it's not just the Registrar or the Registry, it's all of the good guys. It's again spread across the whole stakeholder community as a benefit.

Now, some of this you can't put any dollar value on except to the extent of doing the sort of, you know, impact avoidance mass, the sort of goofy mass but that's okay with me. It still strikes me as something

that we can support in a report. And I'm just, you know, I'm going to shovel a bunch of these that I make up on my own into a draft and let you all shoot at them but I'd be interested to see if anybody else has got ideas to contribute to this pile.

So I'll be quiet and wait for a minute. Go ahead, (Mark).

(Mark Rasmussen): You know for stopping fraud and we were stopping people from getting their money cleaned up out of their checking accounts then they have more money to spend registering domains and buying services from ISPs and things like that, you know, if you want to look for a bad news kind of thing.

Mike O'Connor: Well, and let me rephrase that a bit, it seems to me that there's probably, you know, I was looking at the bad info policies that the affiliates is promulgated and thought about it, you know, I mentioned that Dot-Info as a TLD was getting a pretty rep because such a huge proportions of its domains were being used for phishing and Malware.

And it wouldn't surprise me at all if we can be invisible observers of their managerial meetings if they didn't say at some point, if this domain - if this TLD is perceived as unsafe it's going to make it difficult to sell names in that TLD. We will probably sell more names in that TLD if we can change that perception. I would certainly say that and I wouldn't be surprised if somebody in that group did too.

Now, I'm not evoking huge outpouring so I'll leave this for now but, you know, feel free to either beat me up on the list or privately on this and we'll carry on. (James), go ahead.

(James Ladera): Thanks, (Mike). Just a thought that an indirect benefit would be that if Fast Flux and associated spam and other activities require a degree of organization and coordination between a wide variety of criminal elements and any remediation of that would disrupt those networks thinking Botnet's Malware distribution, spam and a lot of - it just touches on so many different areas that's what makes it difficult to identify and define and solve, but it also makes it - any counteractions, I think, disruptive for those networks.

Mike O'Connor: Yeah, I think that's right. Great. Anymore, last call?

Okay. One more sort of open brain- let me see how we're doing on time here. Oh yeah we're fine. Sort of a brainstorming conversation I'd like to have and then we can carry - we'll carry all these on on the list - would be to throw out ideas about options that we want to propose. We've got a pretty good list starting to build but I just wanted to see if people wanted to float an idea or try something out or anything like that while we're on the phone together.

Maybe we're just real comfortable doing this on the list. For those of you who aren't, you know, the list is of course - the 80/20 rule applies on the list, there's 20% of us that are going a mile a minute and 80% of you are being pretty quiet. Is that okay that it's that unbalanced?

Is it dismay that you're not participating much, overwhelmed, because, you know, the list is pretty productive and it's, you know, all joking aside it does produce an awful lot of email, but there's a lot going on there and I just want to make sure that folks who are either uncomfortable participating in the list or I want to try stuff out in a

different way have a chance to speak, I don't want to just lock you all out.

Sort of take that as everything is okay. Nothing on solutions. I'm not as concerned about that one because we are having a pretty good conversation about that on the Web. I think that's it unless people have other topics that they'd like to talk about today. It seems like we're making pretty good progress on a lot of fronts. I don't really want to get in the way of any of that.

(Robbie): I'd love to ask a general question when we get to that point in today's call.

Mike O'Connor: This is a good spot for that. Go ahead.

(Robbie): Is there a sense amongst the group that the answer to this is to actually make changes to the policy that change what can or can't been done or is the movement towards recommending a system where you make the information available and external parties make their own decisions based on the data?

Mike O'Connor: I think that's a wonderful question. I'm not sure that we've got a sense either way at this point. There are certainly a number of proposals on the table, most of which doesn't require much in the way of policy change. What's the sense from other folks? (Dave), go ahead.

Dave Piscitello: So I'm sort of curious about what (Robbie) means when he says external parties? From my, you know, one of the things we've been talking about today, for example, on email is this notion of, you know,

of an accredited or a list of accredited parties who would be able to have an accelerated path towards the suspension.

And, you know, we obviously have lots to go through before we, you know, we conclude that, but my sense is that policy is too static and what I would like to see in policy is the ability for Registries and Registrars to take on a little bit more responsibility and accountability or, you know, or dealing with malicious acts that involves domain names.

So I would not imagine that a change to an RAA would say you must implement X, you know, I would like to see, you know, like to see something that comes out of the group that says here's a set of best practices and, you know, somehow, you know, create some sort of encouragement or enticement for Registries and Registrars to do that. Now, what that - what would that be? I don't know and it might be that Registries who comply to the best practices only pay 24 cents a domain, you know.

I don't know but that the notion is that there's got to be an incentive for people to actually do this, typically the incentive is monetary, especially if they're going to be spending money doing it. And so I'm just trying to think of, you know- in past whether it's policy - or not yet think about policy, more think about let's get a list of solutions and see what that list is and then see what, you know, what the implications are of not only the individual one but the sum of those.

Mike O'Connor: Great comments. Thanks, (Dave). Other comments on that one? I think it's a great question. And as (Dave) was talking - I'll feel in a little Irish blather while you're thinking.

One of the things that can provide non-monetary incentives is also information. So for example, one thing we could do is suggest that Registries and Registrars and businesses and access providers and anybody else who wants to participate share the information on things like how fast did they respond to a request to take action on average.

And just put a metric of some sort out there that just says, you know, this is a metric that we want to use - it could be voluntary, it could be otherwise but, you know, voluntary seems like a good place to start - and not just track, you know, not just post the average but also post the trend which hopefully would go downward and to the right.

This is ancient Baldrich quality stuff again and it's really back to that which gets measured gets done kind of thing and is a way to get out of the monetary and policy arena and still drive positive change into a system. So there's a thought too.

Other folks got comments on that question, the good one?

Marc Perkel: This is (Mark) and I have idea on that. My idea would be to, you know, using Reg - you know, good Registry reporting techniques that we would actually reduce the burden on the Registry by having systems that makes reporting, you know, easier and keeping the spammers out of the reporting system so that Registries and Registrars want to adopt this because it makes their life easier.

I think that we can come up with (unintelligible) life easier for Registrars and when you make life easier and they are more profitable they're going to want to do it because it makes life easier.

Mike O'Connor: Yeah, I agree. That's the, 'What's in it for me approach', which I like a lot. And maybe that's - I haven't been following the list this morning because I sort of turned off email to get ready for the meeting - but maybe that's what this accredited conversation is about.

One of the things that occurred to me is that - I think (Randy) put up a really good post about solutions late yesterday and one of those was to encourage Registries to instrument their Registry so that they can generate some of this information. I'm not sure that that instrumentation necessarily has to happen at the Registry.

It seems to me that maybe independent organizations can be certified to do that, Fish Tank, Google and that the Registry-Registrar community wouldn't have to pay to build it, they would just simply have to share information. I don't know if that's where that conversation was going but that seems to me to be a way to take some of the cost and implementation burden off of the Registrar-Registry community.

Wendy Seltzer: This is (Wendy) and I get really uncomfortable when I hear about trusted private accredited entities and tools to let them take action that are both outside of public scrutiny and so I would lean towards providing information and letting the groups that exist outside of ICANN and under governmental - other checks and balances and due process take that information and use it, especially when we're talking about criminal activity.

So my preferred solutions would lean towards the informational and even away from the best practice little push because some of those pushes sound like shoves into making the best practices mandatory.

Mike O'Connor: Yeah, I think there's an ocean of gray in there for sure and I think that'll be a good conversation for the list to sort of put some boundaries on what would be appropriate or acceptable and what wouldn't. That's a great point, (Wendy).

Other comments?

(Rod Rasmussen): This is (Rod).

Mike O'Connor: I'm not paying attention. Go ahead, (Rod).

(Rod Rasmussen): I'd just like to take a polar opposite position from (Wendy). Is that (unintelligible)?

Mike O'Connor: I'm sorry we're allowed to have opposite points of view.

(Rod Rasmussen): I should say polar opposite, I understand where she's coming from. But, you know, that's - this is an area of, obviously for me, of critical expertise and unfortunately there's no - there is no governmental agency, authority, whatsoever that can actually effect any kind of mitigation in anything other than glacial speed which is why, you know, companies like mine exist and others in this field and why we've got volunteer efforts and others out there that are trying to do something to mitigate harm against individuals as quickly as possible.

So having a, you know, a process to go through is actually I think preferable to the current situation where we have kind of a Wild West thing going on out there where people are reporting to other people

and if you know somebody at someplace then they'll act quickly for you if you don't, you know, they might not even pay attention to you.

Some people have very defined - well-defined policies as to how to deal with things and other people have none. So actually putting a framework around it, I think, actually helps in the end everybody to create at least a set of boundaries. And then if we want to push the boundaries around based on where, you know, various concerns come in about privacy and due process and things like that I think that that's reasonable.

Right now we're an anarchy when it comes to a lot of the - dealing with the issues that, you know, Fast Flux represents. So anything we can do, I think, to help bring that far better will help out. So - but I think you're right, I think this is a great list discussion because we could go on and on I think for hours debating the type of...

Mike O'Connor: Well, you know, one of the advantages of doing this in conversation is that we can clarify some things. And I want to just check and see with (Wendy) - (Wendy) when you were reacting to what I said, I heard your reaction as be careful of - in giving these external certified organizations this authority and that - and I guess what I heard is sort of a subtext in what you were saying is perhaps to leave that authority within the existing ICANN structure, is that what you were saying or did I misinterpret that?

Wendy Seltzer: Yeah the first part, yes. I don't believe that ICANN has a lot of that authority right now and I believe that it's a good thing that it doesn't either. I think we have court systems lists are the best judges of criminality as it differs from jurisdiction to jurisdiction and we can do

things to provide information that can be used in those processes but I don't want to see us replacing them.

Dave Piscitello: I don't understand how you make the leap from, you know, from an accredited agent to, you know, abrogating, you know, legal due process, every time people do this I just get lost, so I don't see anywhere that...

((Crosstalk))

Wendy Seltzer: But you see if...

Dave Piscitello: ...I don't see anywhere that we have certainly - we have explicitly said "Let's do this completing barring and ignoring the rights of Registrants." I've never seen that in any conversation, (Wendy).

Mike O'Connor: Hang on there. Settle down there, (Dave), you know. I'll intervene as your Chair and ring leader, ring master. You know, brainstorming is great but let's not get annoyed with each other personally.

Wendy Seltzer: I'm not saying this - that we've gone all that way but processes that, you know, privilege one group of parties over others can make it easier to let those privileged parties take away the rights of the masses. And I - we've seen it in the - in some of (Dan)'s (unintelligible) contest and I'm trying to keep us from going down that path with anti-Fast Flux.

Mike O'Connor: Is - I think this is really important folks, so I kind of want to - I'll take an action to kick off a thread on this topic and I want to name the topic because I think - I think if we can put some boundaries on this, that we can all feel comfortable with, that we will have advanced the cause a

lot. Somebody want to put a title on this? I don't - one of the advantages of being the village idiot is I don't know what to call these things, but what would be a good title for that email thread?

Wendy Seltzer: I like 'Due Process.'

Mike O'Connor: You got it. Anybody uncomfortable with that?

Dave Piscitello: It's not. I object to that, it's not.

Man: I agree.

Mike O'Connor: All right. So let's refine that a bit. Keep going. Counter proposal.

Dave Piscitello: I don't see.

Man: How about 'Response Process?'

Mike O'Connor: Response Process. Okay. (Wendy), are you okay with that one?

Wendy Seltzer: Sure.

Mike O'Connor: Cool.

Man: So we're really already kicking the discussion off under the guides of proposed solutions, right (Mike)?

Mike O'Connor: Well, we are and we aren't. I mean what I want to do with this particular one is - again sort of from the village idiot perspective, it seems to me that there is the balance between the rights of the

masses, the individuals - which I think (Wendy) is the advocate for at this point, the needs of law enforcement and others who are trying to mitigate harm. I'll tag (Rod) with that for the moment, although he doesn't have to accept that one.

And, you know, this is an age old discussion and what we need to do is translate - you know, we're standing on the shoulders of giants here people. I mean this is a discussion that's gone on for thousands of years, but we need to arrive at a place where we strike the right balance or at least strike a proposed balance between those forces so that each side has their needs met as best as possible. And then recognize that neither side is going to be entirely pleased with what we come up.

This is like when I use to negotiate union contracts, we always use to say that the contract was good when both of us was equally dissatisfied. So it's not that we're going to come to a conclusion, but I think that discussion of that balance and trying to delineate it is a topic in and of itself that will then help us choose between some of those proposed solutions that are out there.

But I'd like to keep the topic pure in the context of a solution unless we need it, you know, we may need a straw man solution to have that discussion around and maybe the straw man is the certified agent, and if that's the one to trigger it fine, but, you know, not pull all the solutions into this but try and stay focused on that balance.

I'm going to tie that off - I'll summarize all of that in an email and get it out later today in an email side. That was a great question. That was all triggered by the question that came up are we after policy or

information based solutions? Do we have any other really great questions - general questions like that for the group?

Marc Perkel: This is (Mark). I wanted to say one more thing about the accredited thing that (Wendy)'s objecting to. The idea of the accreditation isn't to get an exclusive cobble of, you know, invisible, you know, agencies that control - secretly control, you know, who gets access to domains and who doesn't.

The idea is to, you know, include people who are in the, you know, for instance the servering business, you know, who can send - you know who are processing lots of quantities of email. And let's say, you know, that I detect, you know, a specific domain that's being used for fraud and I start sending in automated reports to Day Daddy and Day Daddy simultaneously is not only getting reports from me but they're receiving reports from...

(Rick): Is it anything remotely possible that this scenario can be shorter?

Mike O'Connor: Now, (Rick) settle down. Look (Mark), it would be good to drive quickly to the point we're getting pretty close to the end of the call here.

Marc Perkel: Okay. Well, the point is, is that you know multiple reporting accredited reporting people, you know, would be out of the same domain and that would trigger the interest of the Registrar, you know, who may make a decision about whether or not to shut down a domain that's being used for abuse.

And the - it would include the - in these complaints the spam that's being sent, you know, that - that is questionable and the idea of it

being exclusive to accredited is not to make a, you know, an exclusive group but to more to keep out so that there isn't a lot of noise in the information so that Registrars can make more accurate decisions.

Mike O'Connor: Okey-doke. Thanks. I'm going to snip this one off at this point because we are getting down to the end of the call. And I'll share my screen again.

(Christian Curtis): This is (Christian). Could I ask real quickly, have we allotted responsibility for someone to kickoff that email thread?

Mike O'Connor: Yeah, I've taken that action.

(Christian Curtis): Okay.

Mike O'Connor: I'll write it up. And then, you know, feel free to beat up my write-up too. I'm not going to do much except launch the thread. I'm not at all an expert on that stuff.

Here's what I sort of put down for our plans for next week. I think we've got a couple to add, which I will, but the ones that I thought of is - I want to remind folks that the original deadline for the constituency input was next Friday the 5th and we slid it out to the 8th. Oh no, it's - it was the mid-week but we slid it out to next Friday.

So just a reminder to ping your respective constituencies one more time and say sort of last chance folks with two caveats, one, remind them that this is just the brainstorming, this is not the react to our suggestions phase yet. And then the other is that I'm growing less and less enamored with the template that I sent out.

So if your responses come back in the template form that's wonderful, if it turns out that it's very difficult to respond and wedge that response into the template just note it and carry on because as our conversation has evolved I think that the template doesn't necessarily work as well as it should. So sometimes these things develop a life of their own and I just want to let you know that at least from my perspective I'm not terribly concerned at this stage if we don't adhere to the template.

Then - I'm not sure - I think wrapping up benefits and proposed solutions sounds like really optimistic so I think I'll just change that to continue. And I think that we'll continue that along with the threads that we've identified and I'll get those out later today, you know, more in the form of the last one resume or carry-on or something like that.

I think that, although the email volume is probably approaching a record for our working group that it's been very good and we've gotten a lot done and we've developed a hell of a body of knowledge and I think that's a great thing, so just a final attaboy for all of us to carry-on and that's what I've got coming next week.

Is there anything else that we need to cover today in the last few minutes? We've got about five minutes before we're supposed to wrap up. I think we're done. Thanks, people. See you in a week and see you on the net.

Woman: Thanks, (Mike).

Woman: Thanks, (Mike).

Man: Bye all.

END