Fast Flux PDP WG Teleconference
TRANSCRIPTION
Friday 25 July 2008 15:00 UTC

Note: The following is the output of transcribing from an audio recording of the Fast Flux PDP WG teleconference on Friday 25 July 2008, at 15:00 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at:
http://audio.icann.org/gnso/gnso-fast-flux-20080725.mp3
http://gnso.icann.org/calendar/#jul

Attendance
Mike 0'Connor - WG Chair CBUC
Mike Rodenbaugh CBUC

Registry Constituency
Adam Palmer - PIR (registry constituency lead)
Greg Aaron - Afilias Rodney Joffe - Neustar

NCUC
Christian Curtis - NCUC

Registrar constituency
Margie Milam - MarkMonitor
James Bladel - Godaddy

Wendy Seltzer - ALAC liaison ICANN Board

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

Staff:
Liz Gasster
Marika Konings
Glen de Saint Gery

Absent- apologies:
Paul Diaz - Networksolutions
Kalman Feher - Melbourne IT
Eric Brunner - Williams - CORE
Zbynek Loebl ISPCPC

Coordinator: The recording - (unintelligible) you can go ahead.

(Mike O'Conner): Thank you (Mathieu).

Coordinator: You're welcome.

(Mike O'Conner): Swing us around.

Woman: Would you like me to do a role call (Mike)?

(Mike O'Conner): Oh yeah. You could do that.

Woman: We have on the call Mike O'Conner the Chair, and Dave Piscitello Christian Curtis. Wendy Seltzer although her name is written (Soldier). Margie Milam, James Bladel and Adam Palmer. And from staff we have Liz Gasster and Marika Konings .

(Mike O'Conner): Thank you. I think Glen gets the arriving close to the meeting panic award for the week. Arrived at her house about five minutes before the call started, so pretty good.

Okay. So I'm getting better at this folks. So I have the agenda up on the Web site. You can take a look at. We've done the roll call. Thought we'd just take a look at this agenda, then I've started the status reporting cycle. That was one of my - and we'll go through that really quick.

We'll take a look at the action items from last time. They're actually aren't any updates to the interim report, but I've got a document that I'm working on that we'll work on in lieu of that.

Session topics - I don't want to nail down the definition - pick one. I want sort of come back around to the data thing. That'll actually come up in the action items. This is a little out of order. I too arrived five minutes before the call started, so this isn't my best crafted agenda of all times.

The document I want to go through is the impact document. That's also a repeat. We can figure out any other topics we want to talk about. Figure out next week. And I think that's okay.

Woman: If somebody could paste the URL into the chat then it would be easily accessible.

(Mike O'Conner): That - come.

Woman: Thank you.

(Mike O'Conner): You're welcome. That's a great idea. I'm learning more new toys. I tell you this project has given me more gizmos to fiddle around with. Adobe thing I think is really - okay.

So, let me take us to the status report. All of this you can also get to off of the (best luck's) page itself. Our first status report is right there. Let me just step you through what this is all about.

The really simple status reporting thing that I've been doing for I don't know how long, but a really long time. And the first part up here is - if all of the answers to all six of these questions is null, then you as an executorial type can basically close your eyes on the rest of the status report.

Because it means that your leader is saying everything is fine, nothing is off track - take a nap. If on the other hand there's a yes, then down in the bottom area - issues and concerns, there's got to be a little documentation that says what are you talking about?

And we have two yes's, neither of which are earth-shattering, but worthy of note. The first is that the registry constituency requested a delay in getting the first round statements back. That's to the (AIDS).

So I'll post a note out to the whole list for everybody who's going back to constituencies, so shift that date back. I don't think that's going to have impact on the overall schedule. It's just going to make (Liz) and me work a little bit harder. Because I'm going to take the slack out of (Liz) and my budget. So (Liz), without asking your permission, but we're okay.

Liz Gasster: I noticed that. That's okay.

(Mike O'Conner): The other one, and this is one I want to talk about today. It came up on the last call. I listed to the call again. I highlighted it. And that is that (Rob) was lobbying for taking the word fast out of (fast blocks) and on further reflection I sort of want to come back around and at least highlight that as what could be a huge scope increase.

Without (fast) in there we start not having very many boundaries we are working on. So I just want to spend a minute on this call and sort of walk through that discussion again.

Other than that, no news of excitement on (long fine). I pasted our action items into the accomplishments this week. And that concludes the status report. So, I'm going to carry on. Go right into those action items. Sort of find out where we're at.

Dave Piscitello: So are you starting with the, you know, should it be (fast)? Or should it be?

(Mike O'Conner): No. I'm going to start with these action items. And then we'll get to the scope thing in a minute. But I want to sort of take a snap-shot on where the reach out for data effort is. Especially the one to the anti-fishing working group. Did you get anything back yet on that?

Dave Piscitello: Well we actually got three or four feeds of information. One from some - one of the people who is - works in the male anti-fishing work group with the Internet security operations and infrastructure group - the ISOI.

(Mike O'Conner): Okay.

Dave Piscitello: And we got some information back from - it's a learns in some list. And we got some from a university study. But as (world) - we actually have four or five offers for information. And the offers - so the different pictures and different information that we still have to digest. So it's not like we can, you know, we know exactly what to say yet.

(Mike O'Conner): Okay.

Dave Piscitello: And most of this is not going to come in the form that we - that (Rob) had solicited. It's going to be, you know, largely raw data. So we're going to have to take the raw data - I mean, I literally have like a database of 14,000 fishing domains that are achieved. You know, and illustrating, you know, the one database that I have has 14,000 domains and the numbers of times that - and the addresses that we - that were used for that domain in a month. And the ranges were from like one or two to 1,700 in a month.

(Mike O'Conner): Okay.

Dave Piscitello: So, you know, we have to sort of figure out how we're going to kind of treat this in the aggregate as we promised. And distill it into the kinds of numbers that we want to present to the community.

One question I guess I would - I still have is what is it that we want to present to the community? Just some, you know, statistics to corroborate the claims? Or, you know? And then, you know, identify, you know, in the month of, you know, for example, in the month of June 2008 there were 14,000 - out of 14,000 domains that were identified as fishing domains, the median, you know, number of changes to an IP address was (unintelligible).

And the maximum was (bar). And, you know, the locust seems to have occurred around this number. You know, I think, you know, I'm not quite certain, you know, what are the numbers that are - or what we want to use the numbers for yet.

(Mike O'Conner): I think there are a couple of uses. Clearly one is answering the question is this a problem that needs elution just yet? Is it a problem that's rapidly growing, but there's - and there's watching, but isn't huge yet? I think there's sort of scale kind of question. You know, how pervasive is this? How rapidly is that increasing?

And then there's the second part of what you were saying is - and the second part is completely obliterated by that cool sound. Just completely wiped out my train of thought for a minute. Oh, is, you know, we may have to sort of either arbitrarily or with information establish some sort of threshold that says this number of domain name changes in a month is what we're going to consider volatile.

And, you know, so it would be full to have some information that sort of gives us a sense. Because a lot of the descriptions, the (TTL) being 90 seconds means that, you know, implicit in that is that's a lot more than a 1,000 domain IP address changes in a month.

Can't do the math right off hand, but you know, that's more like a 1,000 in a day. And so, I think it's useful both in terms of scope and nature these numbers to give us a sense of what's going on.

Now we have another database from - forgotten his name, the fellow that (Joe) put us in touch with that worked for a network security company - (Atlas). I think there were 10 or 12,000 names on that list as well. Is that the list that you're talking about? Or do you have another list in addition to that?

Dave Piscitello: Let me see where I got my list from. I'm looking - pulling it up right now.

(Mike O'Conner): I got one by email from (Kent). I will have totally bewildered you as often.

Dave Piscitello: Let me - emails.

(Mike O'Conner): I think that the one I have doesn't have - so I think it's a different one. The one I've got is just domains and the date that they put in there database. It too is about 10,000 names that they're monitoring. But they're not calling them best (flux) necessarily, they're just domains that they're watching right now.

(Randy): Hello?

(Mike O'Conner): Go ahead.

(Randy): Sorry (unintelligible). Sorry I joined you late.

(Mike O'Conner): Hey (Randy). They didn't announce you.

(Randy): Yeah that's all right. I came in late, so that was expected.

(Mike O'Conner): That's good. Actually I kind of like it when they don't announce.

(Randy): Yeah me too.

(Mike O'Conner): It's pretty disruptive. It's great to have you on board. We're actually talking data.

(Randy): Okay.

(Mike O'Conner): And matter of fact sent (Dave) on a - perhaps a fools errand. Sorry about that (Dave).

Dave Piscitello: That's okay. I mean, one of the sources that we had from (ABC) was from - and I took the lead paper that was written by (Venoxy Vista) - Indiana.

(Mike O'Conner): And I posted a link for that on.

Dave Piscitello: So that's up and available. I'm looking for the others now. Where'd this come from?

(Mike O'Conner): Well, I don't want to tie everybody up with that.

Dave Piscitello: Right. Well I have a better idea of what you're looking for and I think that (Rob) and (Greg) and I, you know, who are sort of trying to gather this information have to decide, you know, how we're going to actually, you know, compose the kind of statements that you're looking for.

So, what you're telling me is that people still don't believe that this is a problem. And we have to present information to convince them that it is so.

(Mike O'Conner): I'm not sure that that's quite right. I think that, you know, I'm still with my little risk manager hat on here and saying look there are a lot of problems out in the world. And if it happens a little bit the odds are really small. Especially if the fast sub-set is even smaller.

Dave Piscitello: Well I think that one of the problems here is that unless you explain the kind of metric, you know, that signifies large or small, it's - we have an

issue. For example, if there are 200 million domains and 10,000 are being used in a month for fishing, is that a large number or a small number?

(Mike O'Conner): Well it's certainly a small proportion.

Dave Piscitello: Right. But - right. But if those 10,000 domains are costing $1 billion a month, is that a large number or a small number?

(Mike O'Conner): If we could come up with that number - the costs. I'd be just tickled to death.

Dave Piscitello: Okay. So, the reason why I'm doing this sort of Socratic dialectic is because the problem with trying to come up with numbers of that sort is that by and large financial institutions are not particularly willing to share how much they lose with researchers.

(Mike O'Conner): Right.

Dave Piscitello: So coming up with the second number is much more difficult.

(Mike O'Conner): Yeah I agree.

Dave Piscitello: And the other is that if you go out of the raw financial loss into the reputational harm area.

(Mike O'Conner): Right.

Dave Piscitello: It's even harder because it becomes a very soft kind of, you know, numerical analysis.

(Mike O'Conner): I know. But I think that we still need to make the effort. I'm not.

Dave Piscitello: No I'm not saying that we don't need to make the effort. I'm just asking you to tell me what the statistics or the metrics are that you want us to compare. Because if we don't have those it's very difficult to try to make some analyses.

(Randy): Am I still on mute here?

(Mike O'Conner): Say again?

(Randy): This is (Randy). I was asking if I was still off mute.

(Mike O'Conner): No you're not.

(Randy): Okay. Well after I get finished, tell me how to put this on because I can't mute my phone for some reason. Have we gotten in touch with (Team Camry) by any chance? I know that they've done some estimates of some past (lux nets). In particular, the storm worm. And I seem to recall the word millions of hosts infected.

The other estimates I've seen have been 100s of 1000s. As you know, that particular worm's had some real difficulties in size estimations. I do know that in July of last year, I found 16,000 rogue name servers on the storm network. All in broad band connections.

(Mike O'Conner): Right.

(Randy): And that was a huge number out of a 100,000 storm worm potential IP addresses that I tested. I have 600 storm rogue name servers that I gathered in the last oh until July 18th I gathered about two weeks I got 600.

(Mike O'Conner): See I think all of that is useful. Right now we're sort of in a vacuum.

(Randy): Yeah.

(Mike O'Conner): And it would be hard to know.

(Randy): Difficult.

(Mike O'Conner): I'm sort of giving you a bad answer. Because in a way, not being much of an expert at this I'm sort of in the I'll know it when I see it mode. And that's not a good answer for you.

On the other hand, maybe there's somebody in the expert community who can help us categorize this threat across the spectrum of threats.

Dave Piscitello: Well here's another statistic. And tell me if this - one of the problems I have is that I'm not quite certain whether the community that we're going to actually talk to is going to understand some of the (unintelligible).

So for example, I have one statistic here that says we have - we discovered one (unintelligible) that actually results to IP addresses and 365 different (ASMs) - (autonomy) system numbers.

Which means that the reach of that particular flux network is literally global. That there are bots - or compromised computers comprise, yet are part of this network in 365 routing domains. Routing domains meaning something operated by a public service provider, or a backbone provider or an access provider, or a network that's sufficiently large in an enterprise or institutional capacity to be assigned a - what is called a (BGP) or a boarded gateway protocol autonomy system number. So that's an astonishing footprint.

(Mike O'Conner): Right. But if it only happened once, you know, it's partly, you know, how wide? But it's also how deep.

Dave Piscitello: Well, it happened once this month.

(Mike O'Conner): Right. But even once this month doesn't get me real excited. (Margie's) being real patient. (Margie) go ahead.

Margie Milam: Sure. I know there's a lot of studies out there on how much, you know, losses are associated with fishing. I mean (Gartner) and, you know, some of that information's already kind out there in the public.

Is there a way to intelligently, you know, filter that data down from the experts, you know, if the total fishing problem is, we know, whatever $3 billion in the US. You know, what percentage of that is attributable to (fast flex)? I guess that's a question for the audience really.

(Mike O'Conner): Well that's the kind of thing that I'm sort of groping for. Is something other, you know, what we seem to have right is now is a lot of sort of anecdotal evidence. And it makes me nervous to do a policy on anecdotal evidence. I'd like something a little bit sturdier than that.

Dave Piscitello: Well especially with something like risk management. When you're looking at - I'm sorry.

(Mike O'Conner): I'm going to try and grab control of this meeting. (Wendy) go ahead.

Wendy Seltzer: So, I want to get back to the definitions though. I know as much as we hate talking about the definitions. Because to me, knowing how much loss is associated with fishing is almost entirely independent with what's the problem that we're here.

(Mike O'Conner): Yeah. I think that's right. That's part of the reason I'm dragging us back to definitions. Because if we drop fast out of the definitions so that our, you know, I like (Randy's) stuff a lot. And if we took volatile out and just said it was compromised host networks. We suddenly have the whole fishing universe in front of us which strikes me as a huge scope increase.

Dave Piscitello: But why would we take volatile out?

(Mike O'Conner): (Rod) was talking about how last week - on last week's call. How some of these networks behave exactly the same way except they don't do it fast.

Dave Piscitello: Right. But that's still volatile. It's not an inert network in the same sense as any enterprise network like a DuPont or a Fortune 1000 Company's network, or a network run at MIT or College of Charleston is a static - relatively static network. But the notion of, you know, of a volatile network in my mind is one where the host, the routing, the addressing, the name service are all, you know, in a state of flux so to speak.

Where as the notion of, you know, of an enterprise network strives to be exactly the opposite of that. You want, you know, you want stability in your naming service. You want stability in your routes. You want stability in your availability. You want to know and enumerate every host and what activity's going on in those hosts.

So I don't see that taking the word fast out of the equation immediately says we're talking about every fishing domain.

(Mike O'Conner): I think what we need though is the sort of (domically) is that tells us what's in-scope and what's out.

Dave Piscitello: So, can I offer a slightly different interpretation of taking fast - taking the word fast out of flux?

(Mike O'Conner): Sure.

Dave Piscitello: You can say that what it does is change the scope, or you can look at it and say that a year ago our understanding and classification system was course. Because we didn't have the same degree of insight into the behavior of the networks that actually use a fluxing technique.

Having a year's more experience with anti-crime, with anti-fishing, with other investigatory methods with academic research and intense data analysis we have - we understand more about the fact that these networks may have begun with (sass flux) because - or begun with fluxing addressing quickly because that was convenient and it was opportunistic.

But as counter measures have improved, you know, they have adapted to, you know, to become more resilient against the possibility that someone has actually put in those counter measures. And so, by changing the behavior from fast to slow, or by changing the behavior from, you know, command the control centers to distributed command and control center, or to adaptive, you know, instantiation of a control center when one is detected and taken out.

What you're seeing is, you know, that there's an agility here. And that - and by only looking at something that has short times to live as the single nail that we want to put in the, you know, put in the coffin. We are probably narrowing the scope. And I think that was more a fact, or an artifact of not understanding the problem as broadly as we do now a year ago.

(Mike O'Conner): Yeah. I can understand that. So, I think where I'm still at is, you know, I think we need to get to a definition. You know, that we all - I mean I think (Randy) took us a long way with his deconstruction of the thing. Is (Randy's) volatile compromised host network enough of a fingerprint to constitute the definition? Are people comfortable with that? Because if it is maybe we could flush that out a little bit with whatever the attributes of that are.

(Randy): This is (Randy). Is (Eric) on the line? Because I know he and I had a slight mail exchange where he may have had some alternative definitions.

(Mike O'Conner): Yeah. (Eric's) not on today.

(Randy): Oh. That's a pity.

(Mike O'Conner): Yeah that is a pity. I'm sorry. There was that and that was.

(Randy): At the time I seem to recall him talking about re-purposed computers instead of compromised hosts. But I'm going to do him a disservice. Perhaps we can elicit some comments by email.

(Mike O'Conner): Yeah.

Dave Piscitello: I think re-purposed is a hugely broad categorization.

(Mike O'Conner): Yeah.

Dave Piscitello: And it is - I think it adds more ambiguity to the issue than clarify.

(Randy): And one more point and then I'm going to go on mute again. With the compromised host networks, we also are including servers where's there's been some kind of server compromise. And we'll see this through URLs that were fairly easily adapted at working with.

Typically we're able to contact the owner of the network or the computer and then they'll resolve the issues. Where as fast flux, it's a matter of being able to contact people - or actually not being able to contact people.

We just cannot make notices to all of the people who are infected just because it's just so huge.

(Mike O'Conner): (Okee dokee). Well, we need work on this. Sort of a pain in the neck, but I really think we need a crystal clear definition of what we're - because that will also (Dave). (Unintelligible).

Dave Piscitello: I can't hear you. You're mumbling. Sorry.

(Mike O'Conner): Sorry. I do that sometimes. That definition is also going to help with the fact gathering. Because then we'll be able to say okay we want to know about these critters whatever they are. So can we take as a pretty high priority? Say again? Somebody want to jump in? That was a funny thing.

Carrying on. Can we take as an action to really work on the definition next week? Because we got to get this straight folks or we're going to run everybody in circles.

(Rod): (Mike) this is (Rod). I've been listening for quite a while. I don't think they announced me either. Unfortunately I'm mobile at the moment. I will shortly be at my office, but let me try to interject something here if I can.

(Mike O'Conner): Go ahead.

(Rod): I think the central problem we have, and (Randy) discussed on it. The central thing we're trying to look at, or at least as far as back as initial discussions about putting some sort of (PDP) on this were looking at the heart of the ecosystem of the criminal enterprise here using, you know, domains that are registered and put on these networks. Whether fast, slow what have you.

But where the - basically the only practical way of tooling the network is to get the domain name removed by a domain registrar last registry. So there's a central nexus point where there only, you know, kind of real center involved as a domain registration sort of provider of some sort.

Because they're moving them around automatically using the (DNS) system. And the, you know, still - in looking at definitions, if we can concentrate on that. First is the situation for example, where somebody registers a domain name and leaves it on the original hosting company or original registrar's services. Those are easy to deal with. Or fairly straight-forward to deal with. Or they have a domain that's been compromised because they've taken over a server. Those are straight-forward to deal with.

The problem we have is with the fast flux networks that you cannot talk to a key systems operator, you have to talk to literally millions of systems operators. And even then, if you get a hold of them, because this flux thing is (unintelligible) flux thing quickly, they can't even see that they've got a problem.

So it all comes back to the domain registration provider who has a criminal who has reregistered the domain name to their service. Or is trying to register a domain name to their service - looking at the preventative side.

(Mike O'Conner): Right.

(Rod): I think that is really what we want to concentrate on is that form. And what is that? Well, usually it's automated in some fashion. Or it's, you

know, so fast - quickly done by humans that it may as well be automated. So, I think that's really what we're trying to get after here.

Because that's where, you know, frankly (PDP) could apply is there's a domain registration entity involved in the process, that's where policy could actually make a difference.

Otherwise we're just looking at, you know, steps process and other things for ISPs. So if we're going to develop consciously we need to concentrate there on that.

(Mike O'Conner): I think that's informative. I think we need - I still want to beat the heck out of this over the next couple of days in email.

(Adam Palmer): This is (Adam Palmer). Could I jump in for a comment?

(Mike O'Conner): Go ahead.

(Adam Palmer): I'm sorry I can't get online, so I'm not able to indicate my hand up.

(Mike O'Conner): That's all right. For those of you who can't get online, but barge right in whenever I'm talking.

(Adam Palmer): Well I apologize for my rudeness. I did have one comment I really wanted to say in response to, you know, what (Rod) said was that, you know, I think there should be some clarity of, you know, of staying focused. I do think, you know, we can easily get a far feel looking at the wider fishing problem.

And, you know, it might be worth while to focus on why this is necessarily different than any other, you know, kind of abuse. Such as, you know, spam or farming or malware. You know, that takes advantage of the (DNS).

You know, and I think there should be some clarity. I guess I have some disagreement at least to some extent on the ability that (Rod) mentioned of, particularly with the registries of our ability to effect any change here.

And I think that it might be important. I think it's something we'll try in our statement I think - or at the registry constituencies trying to work on, you know, making clear is, you know, to what extent that in fact a registry has any ability to effect change on this area.

You know, whether it's appropriate to sort of suggest that they do, when in fact they may not. So I really think we need some clarity on the effectiveness on that. And whether or not that's an appropriate resolution.

And I want to be mindful sort of of the narrow scope of what I can - could or could not do for this process. And, you know, maybe approaching this certainly in a best practices mode rather than, you know, stepping forward and saying this is, you know, really what - this is what a registry can do. If in fact it can even do it. And this is what we're recommending.

So, you know, just sort of being mindful of some of those points I think would, you know, be prudent as we move forward.

(Mike O'Conner): Thanks (Adam). Let me extend that same invitation to anybody who's not on the Adobe thing. If while I'm talking, feel free to interrupt and get on the conversation.

I want to - (Adam) I think you're right. In a way though, I want to make the distinction between the problem and proposed solutions. In a way, what (Rod) did, which I think might have evoked your comment is he narrowed the problem down to a point where there was really only one venue for proposed solutions. And I think that's an interesting conversation to have. I don't know that we can drive it all the way to ground on the call, but let's separate.

(Adam Palmer): That's not my intent (Mike).

(Mike O'Conner): Okay. Go ahead. Good job interrupting. I did see your hand up.

(Rod): My hand? This is (Rod). My hand better not be up.

(Mike O'Conner): You're trying to get in the room.

(Rod): No, no. I'm still in my car. That's somebody trying to (argentous) me.

(Mike O'Conner): Didn't realize we had two (Rods). Sorry about that.

(Rod): Oh okay. The - really from the roles that different entities can play, and I'm not trying to define those. I'm just trying to actually narrow the scope of the problem statement into these are the kinds of domains that are the issue here. Not necessarily this the only way we can address the issue.

I want to keep out the compromised servers that are being used directly and things like that. So we can actually concentrate on, you know, manipulation of the (DNS) in order to maintain a fraudulent site.

And not necessarily fishing. I don't think this was - the whole purpose of this was for fishing. I mean I think we're looking at entire malicious use spectrum here. I just want to try and get some sort of definition around it.

So, but I'm certain - don't want to put words or solutions in place based on the problem definition. But really just trying to say okay are you using (DNS) in this way to keep these thing alive. And, you know, the real world touch points are usually domain registrations of some sort.

(Mike O'Conner): You know, I think we're - I'm delighted that we record these calls because I don't have to take notes. I can go back through the call later and sort of extract tidbits.

What if I - is there anybody who wants to get an idea into this conversation, so that when I listen to this again, I'll extract it and put it in? If you do, this is a good time to inject it.

And what I'll do is I'll make an action to go through this part of the call very carefully trying meticulously pull out the concepts that we've put forward. Built a straw man definition. Get it out on the Web site for people to.

(Adam Palmer): (Mike) it's (Adam). Just to clarify I guess then my comment. I just wanted to suggest that we, you know, I think it's very important when we're focusing on the problem and not to necessarily prescribe

solutions or suggest that we have this group - it's appropriate for this group to propose or examine potential solutions and not to get out of scope into a wider forms of abuse.

I guess my suggestion, and others, you know, may disagree is at least that this is a focus on fast flux. And that looking at that problem. And not to prescribe any wider solution or policy suggestion would be, I think probably beyond the scope of what we're being tasked to do.

(Mike O'Conner): Would you take (Rod's) narrowing to the (DNS) both sides of the (DNS)? Oh that's our operator. Hey (Matthew). There we go. I think (Matthew) forgot to mute.

Would you take (Rod's) notion that we kind of zero in on the (DNS) kind of things. Not necessarily just (GTL), but the whole domain ecology as our focus? Would you take that as a friendly amendment to your?

(Adam Palmer): I would say actually it's probably - I don't know if any of my colleagues who are a little more - have a sharper technical understanding of the problem than I do might be better to comment quite honestly on, you know, that focus.

But, you know, I've no problem at least with the general best practices sort of approach. Even if we want to sort of go that far for mitigating this. You know, again, I just want to not get into the point where we're sort of defining these are the solutions and this is - and making recommendations for that.

(Mike O'Conner): Yeah. I'm going to be very careful not imply solutions when I extract. I may pull those out and put them in another pile that we can consider later. But I will try not to get solutions defined in the definition for sure.

(Adam Palmer): Okay. I'm not trying to bring this call to a halt, so I think I've made my point. Appreciate allowing me to say it.

(Mike O'Conner): Who's (M Perkel)? (Marc)?

Marc Perkel Yeah hi. This is (Mark). Yeah I guess I'm a little bit confused. I guess you're talking about not defining, you know, coming up with solutions as part of the definition of the problem. Is that correct?

(Mike O'Conner): That's exactly correct.

Marc Perkel Okay. But there is going to be, you know, a solution phase to this, you know, thing. Because I tend to focus more on figuring out solutions. And some of the things that I don't yet know, which in the realm of possible solutions is the ultimate. What is it that can be done?

You know, is it ultimately that if we detect a criminal enterprise using a fake domain that registrars would disable the domain. Is that part of what we're assuming?

Or I guess we're also assuming that we can have some type of management over the rate that (DNS) can not be allowed to change? You know, we could also perhaps, you know, just recommend, you know, information about domains through, you know (DNS).

I mean I guess I don't completely understand the scope of what the possibilities of things that can be done. And maybe I'm premature on this question. But, you know, to figure out what tools we have to work with. You know, that's within the scope of what, you know, this group and I can and can't do.

(Mike O'Conner): Right. You know, I'm going to sort of cut you off being the rude guy that I am. And say that I don't want to stop the conversation about solutions, but I don't want to have it now. Because until we know what problem we're trying to solve we can invent...

Marc Perkel I understand.

(Mike O'Conner): ...solutions to the wrong problem. So I'm really interested in nailing the problem statement. And then once we've go that crystal clear several good things happen.

One is we can zero in on solutions that solve that problem. And the other that is the thing that triggered all this is that then we can go out and capture data that helps us support our conclusions. Which is, you know, especially (Dave), (Greg), (Rod) are out trying to pull together some data that we can use to justify things.

(Randy): (Mike)? This is (Randy).

(Mike O'Conner): Go ahead.

(Randy): Just a short comment. I really would like it if people would try to tear apart those definitions. Because I have questions about some of the wording and some of the implications.

(Mike O'Conner): Yeah.

(Randy): So please, please feel free to destroy them.

(Mike O'Conner): Yeah. They'd go for anything that I write.

(Randy): Yeah.

(Mike O'Conner): But right. You know, I think that what I want to instill right now is sort of a spirit of puzzle solving. And I don't want to make it seem like this is negative or bad. I think this is really important. And hopefully kind of fun as we figure out exactly what it is that we're going to try and solve before we get too far down the road on the solution side.

So, you know, I'm with (Randy). Let's engage in a spirited conversation. I will summarize this part of the call into something. I'll get it out as quick as I can although I'm meeting and travelling all day today. So, it may be pretty late tonight before I get it done.

I'm feeling a pretty high level of urgency to get this nailed so that we can sort of hang on to our schedule that we made. We have this major schedule blow out if we can't get to the end of this pretty soon.

Anything else that people want to inject into the problem definition conversation before we move on? Okay. Well, (Christian) go ahead.

(Christian Curtis): I just wanted to mention that in defining the scope of the problem it might worthwhile to look at the scope of the problem - the scope of the problem that is within ICANN's ability to address - for which is

appropriate for ICANN to address. Versus, you know, generally malicious practices on the whole.

Because I don't want to take good definition of the problem that's going to give the impression that we're going to be able to completely stamp out all malicious practices on the Internet.

(Mike O'Conner): Yeah that would certainly make us heroes if we were able to do that. Is that a friendly amendment for folks? You know, I tend to agree. And I think that in that case, a little bit of conversation right now about what those limits are would be helpful to your summarizer. Any of you want to take a stab at that?

Dave Piscitello: Well if we're going to talk about what ICANN can and cannot do, then it falls squarely in the realm of the operation of the domain name system and registration services.

It doesn't involve routing. It doesn't involve end-point security. It doesn't involved in part, ISPs unless they, you know, they are, you know, accredited registrars.

So, you narrow the scope fairly considerably when you make that statement. And I think that that's probably a good thing.

(Mike O'Conner): Yeah I do too. Does anybody want to expand, clarify, refine (Dave's) boundaries of ICANN impact? Looks like you got it in one (Dave). Okay. I'll put that in as - not as part of the definition, but maybe as a related definition. I don't know. I'll figure out something and we can beat it up in the email. That was a good thing folks.

(Adam Palmer): It's (Adam) again. I appreciated (Dave's) summary. And I think it's, you know, again worth making a point of - that ICANN would seem, you know, not especially well equipped or appropriate to necessarily, you know, prescribe any type of solution to some of these issues.

You know, and I think there's a good question of why, you know, I know at least that even before this group was formed - from at least the registry constituency as to why were necessarily even treating it differently. And not having a similar group for all the other variety of problems that are similarly related.

So, you know, I think looking at the scope and understanding the scope of the whole policy process as - is something that we should be mindful of throughout this process.

Dave Piscitello: You know one of the things that I'd like to interject here is there tends to be very much of a defensive reaction to something like a (PDP) where the - not suspicious, but I can't come up with a better word. Where the expectation - that's a better word is that there will be a policy that actually either imposes something or constrains action.

And one of the things I'd like to have people think about is that in some ways policies can introduce more liberal treatments. And more liberal practice by, you know, by a registry or registrar.

And one of the things that we talked about early on in this whole process was is there, you know, is there - are there practices that we can recommend that may work for fast flux? But also have, you know, have a generous ability in terms of, you know, to quickly diagnose and act independently as a registry. You know, and take down a site. Or

suspend a registrar. Or act without, you know, without some expectation of, you know, of some, you know, penalty or some loss as a result of a contractual breach.

So I really do think that we don't want to necessarily think that anything that comes out of this committee has to be, you know, (close 12) of the, you know, registry agreement with ICANN that says you must do - you must monitor the (TCLs) and they must - and they can't be more than three minutes.

Now I don't expect anything like that in the (PDP). Or in a response that we would generate. And I really wouldn't expect anything that granular in, you know, in a policy between ICANN and a registry.

(Mike O'Conner): I think you're both right. (Rod)? And then (Christian) - well (Christian) are you responding to (Dave)?

(Christian Curtis): Yes.

(Mike): Sorry. Wait a minute I'm going to figure this out yet. (Rod) first.

(Christian): I'm just trying to get in the meeting.

(Mike O'Conner): Yeah. Okay. Sorry. Dang nab it. I wish my eye sight was better. My apologies. (Rod) go ahead.

(Rod): Well actually I wasn't raising my hand. But if you could give me the floor for a second.

(Mike O'Conner): Totally lost control.

(Ed): One thing too is policy may not be something - action you have to take. That perhaps data provided. All right. Because one of the things that we're starving for here is data. And if we're to track a problem, one of the things that perhaps the registry could provide would be data. Or a registrar.

So that wouldn't necessarily be something that was all that onerous either. So that's another thing to think about as we're doing this stuff.

(Mike O'Conner): Good point. I'm going to snip this particular part of the conversation off, just because we are getting a bit ahead of ourselves. I think (Ed) on your concern is well noted. And I will acknowledge it in the minutes.

But I don't want to get us into policy solutions just yet. Because I want to make sure we get our problem statement right first.

I'm going to push this along. We're getting up towards the top of the hour and I'm sensitive to time. The next action item was to go out to legitimate users. And I succeeded at getting through to a couple. I got through to the (C-Level) people who run (Thompson West), the (CTO), the (CSIO) - (CISO) or whatever it is. Anyway, and also got to the (CTO) of a company that runs a very big network, but it's a little company.

And in both cases they got pretty excited about - and were pretty negative about the idea of limiting (TTLs) on hosts. They were less excited about the notion of limiting it on the (DNS) side.

But in the case of (Thompson West Publishing), they set the (CTO) on all of their hosts to 30 seconds. And so, short (TTLs) is something that at least (Thompson) feels they need.

And my buddy (Ralph) who runs this other one agreed that for him to be able to shed load, he needs short (TTLs) on there. He will sometimes go several days without having to do it, but when he is experiencing a lot of load on his network, he really needs short (TTLs) right now.

So I'll write that up. I just wanted to inject that into the conversation real quick. And see if anybody else succeeded at getting out to any legitimate users, and had any observations like that?

(Wendy) did you have any luck getting to any of the folks in the community that you're trying to reach?

Wendy Seltzer: I apologize. I'm going to have to leave in a moment. And still not much definite. Although I did get a few bursts of laughter when I - so, there's a group turning to address some problems by limiting (TTLs). The busts of laughter were hah, good luck breaking every content distribution network out there.

(Mike O'Conner): Yeah. Yeah. I think that's right. I think especially on the host side, the two (cont) distribution folks that I talked to got pretty cranky about the idea of limiting (TTL) on the host side. Especially given the patents that (archaism) got, which.

Dave Piscitello: How did you ask the question?

(Mike O'Conner): Say again?

Dave Piscitello: Can I just ask how did you ask the question? If you ask the question, I mean, you can beg an answer by saying supposed we unilaterally, you know, refuse to allow (TTLs) in the global Internet. They leave in less than an hour. Okay?

(Mike O'Conner): Right.

Dave Piscitello: I can imagine almost everyone who runs a legitimate name service would find some reason to object to that.

(Mike O'Conner): Correct.

Dave Piscitello: If you ask it in the context of some of the things that (Steve Crocker) had mentioned where you'd say supposed what we had was, you know, was a method where, you know, a legitimate use of a short (TTL) would simply require, you know, a request. Or to be provided on a - identified on white list. Would you mind going through the extra steps so that you can help us eliminate seven million, you know, rogue (DNS) servers that are running short (TTLs). You would get a different answer.

(Mike O'Conner): Well I actually asked the question almost exactly that way, except for the last sentence. And the concern that came back is, you know, these guys are infrastructure nut cases as you might expect.

And they don't like to inject anymore points of failure into their process than they can. So they're concern is that the white list, token, (Steve

Crocker) and logic kind of thing would inject another point of failure for them.

And so they were not enthused about it - a solution like that. Because I did in fact not just throw out the notion that we would arbitrarily limit short (TTLs). I knew that would get that response.

But, you know, there's a lot of concern about points of failure there that we'd have to address before they would get very comfortable I think. (Christian's) next. Go ahead (Christian).

Wendy Seltzer: I apologize. But talk to you later.

(Mike O'Conner): Thanks (Wendy) thanks for staying as long as you could.

(Christian Curtis): To some degree we can address this when we start talking about solutions. But it seems to me that - our concern as far as who might be impaired for - if we were to require white lists to where request permission for a short (TTL) might cause problems for new technologies and new uses. And create problems down the line beyond just those that might exist for people already employing the technology.

(Mike O'Conner): Yeah. That's actually my buddy (Ralph) is one of those guys. He works for a company called (Swarm Cast) which is doing some pretty interesting stuff with distributed content distribution. And, you know, he would fall squarely in that new technology category.

I'm going to push this along. I want to remind everybody that we should be out to our constituencies getting those constituency inputs. And

remind folks that this cycle is not as formal as a real formal constituency statement.

So, you know, this is still at the brainstorming input idea stage rather than reacting from a policy standpoint. But, a reminder that we should be well along in that process now. And getting - yeah go ahead.

(Rodney Jopy): (Mike)?

(Mike O'Conner): Go ahead.

(Rodney Jopy): It's (Rodney Jopy). So the other one of me.

(Mike O'Conner): The other (Rod).

(Rodney Jopy): Just twice in just in looking, but there's one thing I wanted to volunteer is I thought about originally is obviously most people see us a registry operator (unintelligible). But are sort of - manage (DNS) business where we're probably the 800 pound gorilla in terms of (DNS) as a service.

So I've got a very large data set of real data in terms of (TTLs) for (DNS) records. (Unintelligible) places like, you know, Amazon and Harley Davison and Staples and Office Depot and, you know, about 8,000 major Internet organizations.

I could probably run some analysis and tell you actually what the average and median and mean (TTLs) are for probably 30 or 40% of the e-commerce world.

(Mike O'Conner): Ewe cool.

Dave Piscitello: Hey (Rodney) this is (Dave). Could you identify specific low key of the data? So for example, you know, if you come up with a median that's fine, but it would be nice to understand - if you have like scatter plot where the distribution is - sort shows that, you know, there's a large concentration of people who tend to use (TTLs) around the 30 minute side. There's a large concentration of people who have (TTLs) that are measured in, you know, three days.

And I think would be actually kind of helpful in sort of trying to understand where the outliers are.

(Rodney Jopy): Sure. In fact, given three or four days what I could probably also tell you, because remember that there's a difference between (Joe's Sushi and Bait Shop) with a 30 second (TTL) and Amazon or MySpace with a 30 second (TTL).

But I can - probably also related to the number of quires of that particular record guests.

Dave Piscitello: That's cool. That would be interesting stuff too. Thanks for offering to do that. Because that (unintelligible) work.

(Rodney Jopy): I'll start that today and I'll probably have something for you guys my Monday or Tuesday.

Dave Piscitello: Wonderful.

(Mike O'Conner): Now that's on the (DNS) server side? Or also the host side?

(Rodney Jopy): This is - so we're authoritative for example for MySpace. So we provide all the (DNS) not just from the - not from the (TLD) point of view, but from the second level downward.

(Mike O'Conner): Oh.

(Rodney Jopy): So I have the records for every one of the publicly facing MySpace devices. Or the Amazon machines. Or parts of Amazon, and for every one of their host records that are publicly facing.

(Mike O'Conner): Wow. That's wonderful. Can you also extract on the (DNS) side? The (TTLs) on their (DNS) server?

(Rodney Jopy): Well I am their (DNS) servers.

(Mike O'Conner): We know that. Wow. Very cool. Okay. Because one of the things that everybody that I talk to said that is that they didn't care at all about (DNS) (TTL).

(Rodney Jopy): Yeah I mean, I have a reasonably large business that people do.

(Mike O'Conner): Oh really?

(Rodney Jopy): And one of the big things is the - is the (TTL). We have some people who have a zero second (TTL).

(Mike O'Conner): On their (DNS) servers? Or on their hosts?

(Rodney Jopy): On the hosts. On the (DNS) it doesn't make a difference because they become a customer of ours.

(Mike O'Conner): Right. That's what the folks at (Thompson) were saying is they were a lot more comfortable with the idea of the (circadian) logic applied to the (DNS) servers and the (TTL).

(Rodney Jopy): This is fine because therefore this is the (testimony) that we just established in terms of where, you know, where are scope ends. We're not really talking about a record or (TTL) for a record for host. We're talking about (TTLs) for, you know, name servers.

(Mike O'Conner): Right.

(Rodney Jopy): And from name serves I don't know that we ever get anyone saying to us - and we're a part of obviously some very big companies that say to us, you know, we want to have a short (TTL) on the name server.

(Mike O'Conner): Right. That's the sort of emerging consensus that I'm hearing too.

(Rodney Jopy): Well that would be a very valuable data point and conclusion from this committee. Because it actually gives us some very interesting, you know, insights into how to monitor behavior.

What I'll probably look at is if I look at the order trail, I could see how often companies at the second level want to change their name servers.

(Mike O'Conner): Oh. That's another good one.

(Rodney Jopy): Because remember that while the (TLD) may actually only have four name servers identified, in some cases, you know, we end up answering an additional section with another four or five name servers that are configured by the customer. I can have a look at how often that happens. And how often it changes.

So it's one of those (DNS) traits where when someone configures a domain or registers a new domain and it's say .com, and it comes over to us. In (com) itself there may only be two name servers - or four name servers, you know, (PNS 1-4) (unintelligible) .net.

But in our system, they can configure additional name servers that get returned. I can have a look at what the, you know, how many of those we have. And how often they get changed.

(Randy): That's wonderful. (Rodney) this is (Randy). Can you also do (c-names)?

(Rodney Jopy): Yes.

(Randy): That would be good.

(Rodney Jopy): Same effect as the groups because people think about stuff now - if you over the next few hours can tell me what you'd like us to look at. Knowing what kind of data we've got. I'll run a project over this weekend with my guys and come back early next week with some hard data.

(Mike O'Conner): Very cool. (Rod) you get the hero of the call award.

(Rodney Jopy): Not yet, but.

(Mike O'Conner): Yeah but I think this is, you know, that this is going to be very helpful. I think both narrowing down the definition a bit as we did in the early part of the call. And then this data to give us some insights moves us forward a lot. So, many thanks. I just gave you an action. Let no good deed go unpunished. That's my motto.

(Rodney Jopy): No that's not problem. I'm happy to do this. Because this research is really interesting. It's something that was never looked at. And I know that because the way our system works, there are many people that add name servers to the records they have configured in our system for them.

And I know that in many cases those name servers have much shorter (TTLs) than the name servers of the registry itself allows.

(Mike O'Conner): Even the name servers? Not just the hosts?

(Rodney Jopy): No the name servers. You can create in our system - you can create additional (NS) records.

(Mike O'Conner): Cool. Okay. For the rest of the folks on the call, you heard him. Get your notes to him within the next few hours so that your questions can get folded into this analysis.

And I think the more clearly we can frame those questions the better. So take some time after the call, formulate questions that would be just extremely useful for you and get them to (Rod).

Okay. Let's see. What do I want to do now? We've got about 20 minutes. And, I'm not sure that I really want to drag us through the document that I created because our changed enough that we would be constantly course-correcting just to accommodate the new definition.

So I think I may sort of get us to - I'm tempted to end the call at this point and let us go off and work on those two things. Rather than beat up the document that I prepared. Because it needs substantial revisions.

Is there anything else that would be useful to people while we're on the call to talk about? Otherwise, you know, I may just build up a little more credit in the minutes bank and wrap this up a little early.

And I have a huge document, but I think it's a waste of our time to review it at this stage. So that takes care of that one. I have a sense of the plan for the week which I'll get out in a minute. So, I'm feeling close to done unless there's other business and any feedback for me. Of course, always at the end.

Man: Well you've done a good job as usual. I'll give you that for some feedback.

(Mike O'Conner): Thank you sir. I think we all are doing really well on these calls. I just want to give us all a that a boy. Because I know that these are hard. I know that there is this sort of, you know, ICANN is an organization that's in a state of dynamic tension.

And I think we're doing pretty well at being open and taking some risks. And I commend you for that. So way to go. Let's keep going. And we will get together next week. I'll get some minutes out. I'll get a definition draft out. Probably both pretty late tonight.

Get your questions to (Rod). And carry on. And thank you. That's it for me. See you.

Woman: Thanks (Mike).

(Greg Aaron): (Mike)?

Woman: Bye (Mike). Thanks.

(Greg Aaron): (Mike) you there?

(Mike O'Conner): Yes I am.

(Greg Aaron): Hi (Greg Aaron) how are you?

(Mike O'Conner): (Greg) you made it. Just at the end.

(Greg Aaron): I've been on for a few. I though we changed meeting times.

(Mike O'Conner): Oh. We didn't did we?

Woman: No.

(Mike O'Conner): We just sent the same dang email again.

(Greg Aaron): I think I am so turned around. I don't even know what's going on anymore.

(Mike O'Conner): Yeah. It's the dang time zone changes. Sorry about that, but.

(Greg Aaron): Never mind. Yeah anyway, I was on.

(Mike O'Conner): Well good. I can send the early part of the MP3 to you. There was a part of the call where we were going like dang, where's (Greg). So, the two parts of the call - the call really broke down into a pretty extended discussion of the definition question again. Because we're still pecking away at that.

And I would, you know, really appreciate you going through the first part of the call and listening to that.

(Greg Aaron): Okay.

(Mike O'Conner): And getting me any thoughts via email would fantastic. I took an action item to go and listen to that part of the call and summarize it. And I'll do that tonight.

(Greg Aaron): Okay.

(Mike O'Conner): So if you want, you can just hang back and then respond to the summary. But if there's anything that you want to inject before that, by all means.

(Greg Aaron): Okay. I'm thinking it'd be better for me to react to something that's on paper.

(Mike O'Conner): Yeah. That's fine.

(Greg Aaron): Or electronic facsimile there of.

(Mike O'Conner): Yeah. And the second half was really the data conversation that you heard the tail end of. Especially with (Rod).

(Greg Aaron): Right. (Rodney) was talking about the (TTLs) that he.

(Mike O'Conner): He sees in his.

(Greg Aaron): (Seneges) as a (DNS) and hosting providing.

(Mike O'Conner): Right. And.

(Greg Aaron): It's important probably for - I'm assuming everybody on the call understood the difference between what he does in a (TLD) zone versus what he does as a (DNS) provider.

(Mike O'Conner): Yeah. We probed that a little bit.

(Greg Aaron): Yeah.

(Mike O'Conner): And because you didn't hear that probing, that gives me a sense of when you came in on the call. And there's one other thing that...

(Greg Aaron): I missed that. Yeah.

(Mike O'Conner): ...came up. And that was that I went out to a few content providers - (Thompson Writers) and a much smaller one called (Swarm Tech) who actually uses a lot more bandwidth than they do.

And they got pretty cranky about the idea of short (TTLs) on hosts. They were less cranky about short (TTLs) on (DNS) servers. And the reason they were cranky about the short (TTLs) - I proposed it in the (circadian) framework, which was you could be white listed and get permission and so and so forth.

And their concern is that that's an introduction of another point of failure. And they're very tender on points of failure. They really don't like those at all.

(Greg Aaron): Yeah. Yeah. Okay.

(Mike O'Conner): There was some pretty - and the same reaction from the small content provider. His problem is that there are a lot of other things that he can do besides short (TTLs). But because of the (aucamia tasks), if the does them, pretty soon lawyers from (aucamia) show up and tell him he can't. So a short (TTL) is a pretty important tool in his tool kit.

(Greg Aaron): Got it. One of the things we'll probably try to figure out is registries. Is clearly outlined for everybody what a registry can do and may not be able to technically do regarding these kinds of issues.

(Mike O'Conner): Yeah. I think (Adam) did a pretty job of raising that point during...

(Greg Aaron): Yeah.

(Mike O'Conner): ...the definition conversation.

(Greg Aaron): We're working on the technical issue within the registry constituency. Running it past the technical folks and stuff. Because what you do at a registry is you put a zone file out there.

(Mike O'Conner): Right.

(Greg Aaron): And it can contain a default (TTL). And most registries - it's a long one.

(Mike O'Conner): Yeah.

(Greg Aaron): It's a long - , you know, a day or something.

(Mike O'Conner): Yeah right.

(Greg Aaron): But then, registrars don't populate shorter (TTLs) into that or anything like that.

(Mike O'Conner): They don't?

(Greg Aaron): Nope. Not in the registries I'm aware of. So, what I'm - what we may see is at least - like in (EPP) for example.

(Mike O'Conner): Yeah.

(Greg Aaron): Which is the protocol used in a lot of major registries.

(Mike O'Conner): Right.

(Greg Aaron): There is no means to do that even.

(Mike O'Conner): Can they do it at the registrar - I suppose they could do it at - the registrars could do it on their own domain servers. But that's.

(Greg Aaron): If they're acting as hosting providers.

(Mike O'Conner): Right. Yeah.

(Greg Aaron): But at the registry level, there may be limitations on what you can do. Because basically whoever's authoritative for a domain name is the one who has control over the (TTL).

(Mike O'Conner): Right.

(Greg Aaron): So, you know.

(Mike O'Conner): Yep.

(Greg Aaron): Well, what we're trying to do is we're trying to frame that - we're trying to write that in a technically accurate fashion and that'll be part of - probably be part of our contribution. And that's one of the reasons why we - we're running it past our constituency. We're going to have our next meeting, and that's why (Adam) had asked for the extension.

(Mike O'Conner): Yeah.

(Greg Aaron): Because technically we want to have that kind of sub-script go through the technical folks next year. We're trying to write in an accurate

fashion and also in a - with an appropriate amount of detail. But also for the general audience.

(Mike O'Conner): Yes. Like me. Pretend you're writing to me the business puke, not the technical folks who are.

(Greg Aaron): Yeah. We're trying to - we have to find a fine line where we can do the popularization.

(Mike O'Conner): All right. Perfect. Well that's great.

(Greg Aaron): And also make sure, yeah I mean, and again, different registries are doing things different ways probably, so. We'll see what we get.

(Mike O'Conner): Okay.

(Greg Aaron): It's good that (Rodney) was on the call. Because then he can talk about his registry.

(Mike O'Conner): Yeah.

(Greg Aaron): And then I don't know if (Vera Site) does anything different. .com and .net probably have a lot of old stuff in them.

(Mike O'Conner): That's right. Well neat. Glad you made it a little bit.

(Greg Aaron): My schedule is crazy.

(Mike O'Conner): Well. I'll give you.

(Greg Aaron): Put me in the minutes as having been.

(Mike O'Conner): Well you're being recorded. You'll be in the transcript for sure.

(Greg Aaron): Okay. Cool.

Woman: Hi (Greg) and you are down in the - on the presence list.

(Greg Aaron): All right. All right. Well for whatever little it was worth.

(Mike O'Conner): It's always great to hear from you (Greg).

(Greg Aaron): Okay.

(Mike O'Conner): We'll see you in a week.

(Greg Aaron): All right. Thanks a lot.

(Mike O'Conner): Yep.

(Greg Aaron): Take care.

(Mike O'Conner): Bye. Well thanks Glen. I think we made it.

Glen DeSaintgery: Thanks (Mike). That was excellent. Yes. Wow. You really do get to things. And what, I mean, an enthusiastic bunch.

(Mike O'Conner): Yeah. I think this is a really terrific gang.

Glen DeSaintgery: Oh yes. And finally enough people who are (unintelligible) regular. And we have experts.

(Mike O'Conner): Yeah.

END