Registration Abuse Policies Working Group
TRANSCRIPTION
Monday 30 March 2009 14:30 UTC

Note: **The following is the output of transcribing from an audio recording of the Registration Abuse Policies Working Group meeting on Monday 30 March 2009, at 14:30 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at:**

http://audio.icann.org/gnso/gnso-rap-20090330.mp3

http://gnso.icann.org/calendar/#march

Present for the teleconference:
Greg Aaron - Registry C. - Working Group Chair
Pat Kane - Registry C.
Michael Young - Registry C.
Jeff Neuman - Registry C.
James Bladel - Godaddy Registrar C.
Richard Tindal - Registrar C.
James Bladel - Registrar C.
Mike Rodenbaugh - CBUC
Martin Sutton - CBUC
Phil Corwin - CBUC
George Kirikos - CBUC
Faisal Shah - MarkMonitor IPC
Gretchen Olive - IPC
Roland Perry
Barry A. Cob
Jeremy Hitchcock - SSAC
Andy Steingreubl

ICANN Staff
Marika Konings
Margie Milam
Geof Bickers
Glen de Saint Géry - GNSO Secretariat

Absent Apologies:
Mike O'Connor - CBUC
Olga Cavalli - NCA
Nacho Amadoz - domini puntCAT
Guanghao Li – cnNIC

Coordinator: The recording has started.

Glen DeSaintgery: Thank you, (Benedetta). So I did the roll call, Greg. We have on the call Faisal Shah, Greg Aaron who is the leader of the call, George Kirikos, Roland Perry, but I think he has disconnected because his line was giving some problems, Jeremy Hitchcock, James Bladel, Phillip Corwin, Martin Sutton, Gretchen Olive, Richard Tindal. And for staff we have Marika Konings, Margie Milam, myself, Glen DeSaintgery, and I see that Mike Rodenbaugh has just joined as well.

Man: Hello everyone.

Greg Aaron: Okay. All right, thank you for coming.

Glen DeSaintgery: Sorry and Andy Steingreubl has just joined as well.

(Andrew Steinglazer): Yes.

Greg Aaron: If you can log in to Adobe Connect, we use that to manage our speaking queues. So Glen is sending around that link again and please log on if possible from your location.

Okay...

Glen DeSaintgery: You should all have received the link by now.

Greg Aaron: Okay, a couple of brief housekeeping items. A reminder to send your statements of interest into Marika and Glen. We are going to be posting those in link off of the Wiki. So if you haven't sent that in already, please do. And if you need any guidance, there was a note I believe. I forget. Was it from Marika or Glen about how to write those?

Man: Marika.

Man: Yes, Marika sent that.

Marika Konings: We can send out a reminder on how it looks so people don't have to dig through their emails.

Glen DeSaintgery: I'm busy collecting those who have sent them and those who haven't sent them, so I will send you that again.

Man: Thank you.

Greg Aaron: And then as a note, as you saw on the list, (Christina) decided to drop out of the group due to another ICANN commitment. And I think that that's it.

The main purpose of today's meeting is to discuss the document that Martin sent out over the weekend. It's called RAPWG Definitions 2009-3-29. If you could take a moment and open up that document, this contains a proposed definition of (abuse) and then a reworking in addition of various categories and what they might contain.

It was made on the list that these are proposed and proposed only. I think that's worth mentioning at this point just to make things explicit. Just remember, everything we do is public and could be quoted by anybody looking at our mailing archives. So it think it's probably good that we say explicitly that these are proposed (and in discussion).

Glen DeSaintgery: Greg, I'm going to try in Adobe Connect to pull up the document.

Greg Aaron: Okay.

Glen DeSaintgery: Or if you know very well how to do it, I'm happy for you to do it as well. Just so folks know that the screens might be changing a bit.

Greg Aaron: I don't trust the loner machine I'm on right now.

Glen DeSaintgery: Okay, I'm going to give it a go, so don't worry if the screens change. We will try to get it in order shortly.

Greg Aaron: Okay, in the meantime, has everyone been able to find that document in your mail?

Man: I have not found it yet. It's Phil. My mail is still downloading from the weekend.

Greg Aaron: Okay.

George Kirikos: If people go to the Web archive, the (GNSO dot) - the gnso.icann.org, they can grab it off the Web.

Greg Aaron: Yeah and Martin sent it on Sunday at 3:43 Eastern U.S.A. Time.

Man: George, (could you go to that)?

George Kirikos: Yeah, if you go to gnso.icann.org, go to the right-hand side. There's a link for mailing lists.

Man: Okay.

George Kirikos: And then there's a link to - under Task Forces Mailing List archives, Registration Abuse Policy drafting team. And then it's the March 29 email. It's a zip file though, which is kind of nasty.

Man: Let's see. (It should be together).

Greg Aaron: Okay, while everybody is accessing that document, Martin would you like to talk about how the three of you put the document together?

Martin Sutton: Yeah, sure. First of all, from the last meeting, it was agreed that we are trying to list down a variety of abuses that we're aware of just so that we can start to put them into various categories - pre-registration abuse at actual registration and then post-registration abuse. There's also an additional one there that you'll see on this list - the main use abuse.

So between the three, I've listed down and tried to define from various sources a definition for the type of abuse that we've seen. So if we look at the first category, Pre-Registration Abuse, this is where we've looked at the recent examples of malware being distributed, which also gives us clues as to which domains that they could potentially use going forward to control those pieces of malware.

So essentially I think without going through them one by one at this stage, we've just tried to apply them into each of those categories where we see that they potentially fit, but also look at who do they affect directly - who is the major target. The reason being here is so that we can at least then start to focus in on some areas of where we could potentially do something (it). Now whether that's within this forum

or not, it can then be decided. Because I think quite a few of these we could probably consider outside the scope of RAPWG.

I think as some of the emails going around today quite rightly advise that you know we need to keep this information and at least show that we've decided what is in and what is out of what we don't consider to be abuse. So that if any subsequent questions arise as how we approach this, that we've actually considered a whole variety of aspects of abuse and have reasoned out why some are excluded and why some have gone through to the next stage where we believe there is some policy (amendments) that we could look at.

Now the other thing I would draw your attention to is right at - the first element is the abuse definition. We are throwing this in to try and at least give some focus as to what we're talking about. The last (call) is what do we actually consider to be abuse in this respect of the domain names - registration abuse policies. And I think that is one thing that we need to look at and agree upon between ourselves as a group and also then look at the particular types of abuses we've listed and agree that - or debate those as to which we think are defined well and should be in there. And I'll just recommend that that's the next steps that we take. Is that suitable?

Greg Aaron: I see James' hand up.

James Bladel: Yes, thank you Greg and Martin. This is an excellent list. I had one question or possible suggestion for another column, which would be for each of these different types of abuse if we could determine which ones are solely dependent upon the domain name system and which ones are equally effective or in the (wild) using just IP (directories)

only. And that might be one litmus test to help us determine which category these go into. And that was just all I wanted to add.

Greg Aaron: Okay, so another column discussing whether there are dependencies and/or - could you say again your note about IPs?

James Bladel: Well certainly some of these - and I don't know which ones, but some of these will require the use of the DNS system as far as a look up mechanism, but others are as equally effective just using IP addresses only and can bypass any (name IP) resolution. And so I'm wondering if by knowing the difference between all of these different examples if that will help us categorize them.

Greg Aaron: Okay.

Mike Rodenbaugh: James, it's Mike Rodenbaugh. I'm just trying to understand that a little bit better. What - James just tell me why you think that breakdown would be helpful.

James Bladel: Well, it would help us to determine which of these can - which of these require the (bad actor) to actually engage in the practice of registering domain names. And which of them may - if they felt that that was for example a vulnerability that would expose their crime, that they could just bypass that entirely and go strictly upon IP - direct IP resolution as opposed to registering the domain name.

George Kirikos: George here. It would be like SPAM for example. It might be an example that you could have it pointing to, you know, 192.0.168. Well that wouldn't be a powerful example, but you don't need a domain name to carry out SPAM.

James Bladel: Right and I think the same could be said for example for botnet control, but you know that's probably evolved quite a bit since I've last took a look at that, but there could be direct IP resolution into an IRC control mechanism for example. But anyway, I didn't want to throw this off track. I just - I'm really appreciative of this document and I just wanted to get a better understanding of which ones require domains to be registered in order to function.

Greg Aaron: Okay. Well and as we explore each one of these in this meeting and in future meetings, we will need to (expand a little bit) of how they are executed and we can certainly explore those issues a bit.

Okay, I see George's hand up.

George Kirikos: Yeah, I was just going to ask whether the - two questions. The purview of this taskforce - could it also include IP addresses from the point of view of ICANN oversees both domain names and IP addresses. And I've forgotten what my other point was, but I will try to remember it.

Greg Aaron: That's an interesting question George. It's something that's not discussed nearly as much as domain names and I certainly don't know the answer.

George Kirikos: I remember now what my other question was. Maybe if we are going to add columns, it's whether we should have a column for whether a beneficial use exists for this certain type. Like if - namespinning for example might have a beneficial use for people being able to find good available domain names or something like that for every category.

Greg Aaron: Okay. All right, Richard.

Richard Tindal: Yeah, I think my comments may be a little similar to George's, so I'm thinking we might want a column that indicates whether the activity is sort of always abusive in our minds or potentially abusive if used in a particular kind of way.

So for example as we look at the first two items there, I can't think of any scenarios where malware or botnet control could be a legitimate use. To me, I think that's always abusive activity. But as I look at the second item, namespinning, I can think of legitimate uses for that sort of activity. So I would put that in the column - that category of potential abusive if used in a certain way, but I certainly wouldn't call namespinning inherently abusive.

Greg Aaron: Okay, (Andy).

(Andrew Steinglazer): I guess I'd like to second that in that looking down especially into the post-registration abuse category here, there's quite a number of these that really in and of themselves aren't directly abusing (things). For example, putting a lot of meta tags on your site that represent (brand) abuse of search engines and can have the potential still (to abuse other folks). But in the absence of search engines, you know it's not clear that that directly is itself an abusing activity. The same with you know a commentary (site) or something like that.

So I'm not - I've been trying to frame this in. I like the fact that we've got this broken out by consumers, brand owners, et cetera, but it's better to talk about at least if we're going to prioritize it as well in terms

of the type of harm caused and what actions has to take in order to be harmed by this.

Greg Aaron: So we have the suggestion to add columns and explanation or examination of whether these are always abusive or may have legitimate uses. Kind of understand the nature of these things and maybe get a little more specific about when they are abusive or when they are not, okay. And James has asked can these be perpetrated using domain names or also through another means such as IPs.

Okay, anybody else have any comments before we start looking through the doc?

Man: I think (Nancy) has her hand up.

Greg Aaron: (Andy).

Man: Oh, sorry (Andy).

(Andrew Steinglazer): No, I was done. Thanks.

Greg Aaron: All right, (Pat).

(Pat): Yeah, the only other thing that I can think of is that you know some of these items are probably going to end up being out of scope for what we're talking about. I mean when you get towards the bottom when you talk about transfer notices and renewal notices, I think that that's probably something that we could list, but I think that may be beyond what we're trying to achieve here. So it would be good to keep track of those things that we think are abusive, but that we believe that are

either out of the scope of what we're doing or within the scope of what we're doing.

Greg Aaron: Yes and back to Martin's question. If we keep a list, at least this will communicate back to people in our report that we did look at these things and then made a determination about in or out or maybe it's best for another group to look (at better).

(Pat): Okay, I didn't realize that that was said earlier. I apologize.

Greg Aaron: No problem. Phil.

Phillip Corwin: Yeah, two comments, which I think you know to further refine what we've already said here this morning.

Some of these - one may or may not be abusive. You have to - it requires further analysis. I mean cybersquatting obviously - there's a UDRP process and whether or not a particular name being used in a particular way is or is not (violative) is something that is open for dispute and you know it may or not be depending on what the panel decides. But even then, some of these - let's say a particular domain is found to violate the UDRP. There may not have been any abuse in the registration process itself for that name.

So there's - I guess I'm saying for each of these, there may be some categories where further inquiry and analysis is required to determine whether the particular abuse actually exists at that domain. And then even if it does, if there is no abuse in the registration of that name, it would seem it's outside the scope of this group where it's quite clear from the charter that actual abuse in the registration rather than abuse

solely arising from the domain itself is what we're supposed to be looking at.

Greg Aaron: Okay.

Man: That's not true.

Phillip Corwin: No, that is true.

(Burke): (Burke) here. Let's say I owned a domain like seeds.com. I have a generic use for seeds, but there are trademarks for that in obscure categories. So is that cybersquatting? Maybe if you're the trademark holder it is, but you know for the 99.9% of people it's a generic term.

Greg Aaron: Okay, well it sounds like we're getting into the specifics - specific line items already. Maybe what I would suggest to do is to start at the top of Martin's document. At the top is a proposed definition of abuse, and we are asked in our charter to wrestle with this issue. So Martin would you like to read out that definition and tell us about how it was drafted?

Martin Sutton: Not particularly, no, but I will try.

I think it was really to put something down there to debate and (essentially flush out) something more clearer. So at this stage with the charter as it was and the discussions that have already taken place -- one at ICANN and the subsequent call that we've had -- this is a position that we've put on there just so that we can try and tease something out.

So at this stage, we've got it down as malicious or wrongful use causing harm or potential harm to registrants and Internet users. Having said that, I think I've got some items on here where we've pushed it out as registrars as well, so you know even that may need to be added in. So I'm interested in other's thoughts around the group just to see if there is a bit of a way of articulating this to be more precise or broader.

Greg Aaron: Okay, if you'd like to have the microphone, please raise your hand. If you don't, please lower your hand in Adobe.

So far, I see hands raised from (Andy) still and Richard. (Andy) you are at the top of the list.

(Andrew Steinglazer): I didn't realize I had to unraise my hand. It's all good now.

Greg Aaron: Oh, okay. All right, Phil your hand is up.

Phillip Corwin: I just lowered it. I had forgotten to lower it. Sorry.

Greg Aaron: And Richard.

Richard Tindal: I am going to ask a question. So Martin in that definition, could you take a stab at defining the word wrongful?

Martin Sutton: No, see I get worried about this stage because I'm in a room of lawyers and legal experts of which I'm not. So I think this is one of the issues is how to phrase that in a way that is broad enough to capture what we probably want to capture, but not restrictive as well because each location may have its own way of - where it's saying laws that it can

apply. So it was instead of an illegitimate use (unintelligible) used wrongful.

Richard Tindal: (Unintelligible) or Gretchen is there anything else that is worth (saying) at this stage from when we were wrestling with what it could be.

Man: Yeah, you know the - what I would say in connection with Richard's statement is that we were looking at that and we didn't want to make it so narrow as to be just anything that's illegal. We thought it should be broader than anything that was illegal, so we felt that maybe wrongful would broaden the scope somewhat and we could bring in more abusive activity that way.

Richard Tindal: So it means causing harm or (unintelligible)? That's the intent of wrongful?

Gretchen Olive: Yes.

Man: Yeah, so it would cause harm. And that's why one of the columns we ultimately put up there, the additional column, was you know who was it causing harm to, who was the target. And I mean that's primarily why we added that additional column.

Greg Aaron: Okay and Jeremy your hand is raised.

Jeremy Hitchcock: Yeah, my comment is on wrongful just because I really don't know what that means. And in the interest of trying to communicate a definition for abuse, I don't know if we should try to take one nebulous word abuse and try to put another one in to define it. I think something like malicious really captures the - you know not appropriate, but

another word that might need to go in there is illegal. So something like malicious or illegal that's causing harm.

Potential harm also - I don't know if that's necessarily a good word to put in there because it's difficult to say who is the one to judge potential and what does that actually mean. It doesn't mean that something is being abused if there's potential harm you know just because technology can always be used for harm in any way. So it's - I don't know if that word necessarily fits in very well.

Greg Aaron: Okay, George.

George Kirikos: I just - sorry. Just on that point - the potential harm is if you look at some of the types of fraud - sorry, types of abuse that are listed there. Perhaps say phishing. You know the act of throwing up a Web site that is purporting to be HSBC and luring customers to that. And that stage, there is no harm done until somebody actually clicks and gives away their information. So in that case, you know we know something is wrong there. So it hasn't actually caused harm, but it has the potential to cause harm. So how would we frame something like that?

Greg Aaron: (Burke).

(Burke): Yeah, I was thinking more that if we're going to have a definition, that it might be wise to put it in economic terms. And in the little chat box I said, "Perhaps an activity that imposes negative effects upon another party," because eventually you're going to do a cost versus benefit analysis for a lot of these types of abuse. And it's the economic costs versus the benefits of that activity, which will determine you know how to prioritize them.

Greg Aaron: Okay, Mike.

Mike Rodenbaugh: Yeah, a couple comments. I agree with people who are a little hesitant to use words like malicious or wrongful or even illegal in this definition. It's a little bit (circular) and (leads to a further definition) that would have to be made. It's the same problem we ran into in the (fast flux) working group at the outset also, which is that you can never really tell whether you abuse is malicious or not because that's judging the person's intent in using the name.

But I like George's idea of framing it more objectively if it's something that is or could cause harm basically. And I would also add at the end rather than just harm to registrants and Internet users, it's also harm to registries and registrars, and other businesses really - ISPs, et cetera. It's not just harm to registrants and users.

Greg Aaron: Okay, (Andy).

(Andrew Steinglazer): Yeah, though at the same time if we're not going to have a problem with that and try to blacklist all sorts of behavior or create policies to block certain legitimate behavior, intent matters. If I set up a phishing domain to spoof my own users to do a test of how effective things are, I'm entirely entitled to do that at least in most jurisdictions that I know of and others are not. And so - or if I just want to (mock up) a page and do a research study or something like that, I can probably do that too with a closed audience. And so intent actually matters on this.

So I don't know how we steer clear of that especially if we're looking to not just define it but actually specify policy mechanisms or actions that people need to take to deal with it. Then there's no way of avoiding that having that granularity.

Greg Aaron: Okay, James.

James Bladel: I just wanted to voice some support and tie in some of the things that Mike was saying as well as George. With this definition, I think that we're trying to establish there is intent that various businesses are affected. If it's targeted at consumers, it's usually theft of dollars or theft of credentials to get the money. With businesses, it can be theft of resources. If it's a brand, it can be diminishment of brand or reputation.

So I think the word we're kind of dancing around in some respects is fraudulent. I put that in the chat room dialogue box there because we're talking about the intent to deceive or personal benefit at the expense of the target. So (hopefully) one of the lawyers in the room can chime in on whether or not that word is appropriate and separate somewhat the word fraudulent from illegal, and whether or not that's stronger than wrongful. So that was just my question.

Greg Aaron: Okay, I raised my hand. This is Greg.

As Mike mentioned regarding some of these same discussions in the (fast flux) working group, what we've found is that strictly speaking, (fast flux) involves some technical practices, which are in and of themselves not illegal, or malicious, or fraudulent. And you know it involves some things like proxy, and use of low TTLs, et cetera, et cetera. And some people who do those things are doing them for very

legitimate purposes. In fact, some large hosting and resiliency providers do those things. The real issue was the intent. Are you doing it to fool somebody, are you doing it to host malicious or illegal content, and those kinds of things.

The other part of the conversation was what is illegal, and we went around about that for a while. Of course, illegality depends upon your jurisdiction. Some things are just illegal in some places, but not others, or are defined differently depending upon the local laws. In some respects trying to find a common definition is impossible because of that. But on the other hand, you can say - everybody can agree that okay phishing is - it's theft. It's fraud. I think everybody could agree that that was illegal.

Now other areas are a little trickier. I mean in general, everybody in the world agrees child pornography is a horrible thing and it's illegal virtually everywhere. The niceties of how it's defined vary by jurisdiction. And so that - you get into these issues of can one party agree to take it down. They might have disputes about whether it's illegal in a particular jurisdiction in this particular case. So those are some of the issues that we wrestled with and I see some of them coming up again.

More comments on the definition. Should we edit the definition? We've had a few suggestions. Should we continue to use this definition and alter it? Is it a useful thing to do? George.

George Kirikos: Well the definition says to registrants and Internet users. Could we agree that it's the third parties at least - like the economic argument that I said was a way of quantifying it. It doesn't need to actually be in

the definition, but it could be used later on. But I think it's more than just registrants and Internet users. Somebody already pointed out registries and there could be other people that we haven't talked about.

Martin Sutton: Can we capture that by Internet community and then do a definition for Internet community, which covers (a lot of layers)?

Man: I like that idea.

Man: It covers everyone already.

George Kirikos: There might even be people that aren't on the Internet yet. I don't know whether that should be counted. You know some people in Africa for example that might not have ISP connectivity.

Greg Aaron: Internet community - well is the idea to define the potential victims? Is that who we're really worried about?

Martin Sutton: Sorry, this is Martin. I think we should. Otherwise we won't know what we're trying to resolve at the end of the day. There's got to be target parties that are identified and that's how we would actually work out presumably some of the economical type issues surrounding them.

George Kirikos: George here. Just that if you know we have registrars and registries that are a part of the process now, then they might think that they are being targeted because they are not part of the group that could experience abuse. That they are always going to be on the wrong side of the abuse, so that might be an issue.

Richard Tindal: This is Richard. I'm not sure we need to be specific on who is being harmed here. (Unintelligible).

George Kirikos: To potentially also - one registrar's activities could be negatively impacting another registrar. That could be considered abuse under the definition. So it could be that we truncate the definition to malicious or wrongful (use) causing harm or potential harm (period) without specifying the targets. That's one approach.

Greg Aaron: George.

George Kirikos: That was me speaking.
Greg Aaron: Oh, okay. Sorry. Okay.

Richard Tindal: So this is Richard again. I'm still not sure what wrongful means. I think we need to be more specific.

Greg Aaron: Okay.

Richard Tindal: I know what malicious means, right. At least I think I do. It means that there's no other purpose for the activity other than to cause harm. I'm not sure what wrongful means.

Man: I think we should just take wrongful and malicious out for now because again, I think it's (circular) - any conduct which causes harm or potential harm to any third party.

Martin Sutton: Now I think we've got a problem that all sorts of legitimate activities could cause harm. I mean I could raise my prices and that could harm someone.

Man: Oh, okay. That's - I suppose.

Greg Aaron: Well I - this is Greg. I can see unintended consequences of actions being an issue. Like certain activities will increase DNS traffic for example and somebody absorbs that and deals with it. Is that harm? Some might - the people who have to deal with it might say yes.

George Kirikos: George here. One possibility is to use the word extraordinary or something that's unexpected - using that, putting that in the definition. But some representation that an activity is out of the ordinary although that obviously causes judges to be raised about what is right and what is wrong - big philosophical debates.

Greg Aaron: Richard's - this is Greg. Richard's question brings up another question for me, which is if something can cause harm, I think then the next question is so what. Is it something that is fair or unfair? Is it something that should be dealt with or not dealt with? And so where do you go? Or I guess it may cause harm, but what does it mean and what's its significance?

Man: Then maybe we have to define the types of harm that we're talking about like financial theft or some sort of personal injury. Is that what you're trying to get at Greg?

George Kirikos: George here. (Maybe the word undo harm) is the way to attack that issue or define that issue.

Greg Aaron: Okay, anybody else. So...

George Kirikos: Is somebody talking? There's...

Greg Aaron: Yeah, I hear something in the background.

Martin Sutton: Sorry, that's probably me. I've got noise in the background here. Hang on a second.

Greg Aaron: Thank you, Martin. So we have a variety of ideas on the table. How do we shape the next definition for discussion or how do we edit this? One way to do it is to try to do it on the call. Another idea is to try to do it on the mailing list where we can write down definitions and see it in writing in front of each other. Does anyone have a preference? Do you want to keep working on it here or should we break it off and try to do it on the list where we can exchange versions? Anybody?

Man: I guess I think Marika or somebody could probably take the comments that we've spoken and the ones that are in our chat room here and come up with a couple different alternatives. It's sort of a jumping off point.

Greg Aaron: Anybody have any objection to doing that and working on it between now and our next meeting on the list?

Man: No.

Greg Aaron: Okay. All right.

Marika Konings: This is Marika. I think there were some different options raised. Would you just like me to list the different ones so people can you know say which ones they like best or start adopting the different ones as I see fit?

Man: I think it makes sense to come up with a few different alternatives from what we said and hopefully you can try to synthesize them into one.

Greg Aaron: Okay and by the way, I see (Jeff Bickers). Are you at this? I see (Jeff) has logged in to Adobe. Are you with us?

Marika Konings: I don't think he's on the call. He's actually a staff person.

Greg Aaron: Okay. Okay, well Marika maybe what we should do then is - there are several different versions - you know suggestions thrown out in the course of today's discussion. Why don't we try to put however many versions you think is appropriate out there and then we can - I mean we're in an early phase. I'm wondering if nobody has an objection, to kind of just start working through them on the list and that we're still in kind of a brainstorming mode here. Can you put out different versions with the different suggestions?

Marika Konings: Yes, no problem.

Greg Aaron: Okay, thank you. So that's our larger definitional issue. And then the sub team very helpfully listed all of the ideas that have come up so far plus some new ones. Why don't we - George I see your hand.

George Kirikos: Oh, just to talk on that last point. If we added more columns to the paper that Martin prepared, we could actually see what might be abusive under some definitions, but not under other definitions. So we got a call for example and it requires intent - it doesn't require intent and things like that. And it might be able to be captured and maybe we could come up with a better definition once we actually see how many things fall under different definitions like after the fact.

Greg Aaron: Okay, actually Marika at this point, would you like to become the owner of this document?

Marika Konings: Yes, happy to take that on. No problem.

Greg Aaron: I only ask because you're so good at it.

Marika Konings: Well thank you.

Greg Aaron: And we have one suggestion to add another column and I don't know what to call it necessarily - at least one more column. Maybe we could call it notes or something, but a place where we can record whether things are potentially malicious and/or not malicious, et cetera. So we should start capturing these kinds of things.

So anyway, let's just for fun - the first one. And by the way, are we scheduled for an hour or can people go for an hour and a half?

Man: I'm good for an hour and a half.

Glen DeSaintgery: You're scheduled for an hour. But if you'd like to go for an hour and a half, it can be done. The call can stretch that far.

Greg Aaron: Okay, is there anyone who has to drop off after an hour?

George Kirikos: We can use the (voting) mechanism if we want to (do a quick) poll or something.

Greg Aaron: Okay, I'll tell you what. If you can - if you have to drop off after an hour, can you raise your hand or hit the checkmark either way? Okay, I see Jeremy has to drop off. (Andy) has raised his hand. Gretchen. Okay, so we have at least three people who have to drop off after the hour. I'd hate to lose you and we did say we'd meet for an hour. So I want to honor your commitment. So I'll tell you what. Why don't we close at - in another 12 minutes?

But in the meantime, let's go ahead and get started on the list. The first item is category Pre-Registration Abuse, and the first example is malware and botnet control - pre-designation of domain names to control malware. And the example is Conficker.

For those of you not familiar with it, Conficker is a piece of malware that contains an algorithm that calculates domain names that could be - that the malware creators could use for command and control. These names are not registered, but during the course of time, the creator can go out and register one or more of these. So these are names that are potentially dangerous, but maybe don't even exist and are not registered yet.

So interesting question - I'll throw it out for discussion. Is this an abuse?

Martin Sutton: It's a potential one.

Greg Aaron: I can tell you what has happened in real life. Conficker is a pretty nasty piece of work and various registries around the world - (detail) these (NCC PLD)s are blocking these names from being registered in most

cases. Most of these domains as it happens are composed of random letters.

So in most cases, they are names that people wouldn't normally want to register anyway and they don't exist in the registries. In some cases, the names though are as short as four characters, which means some of the names in the algorithm already have been registered by various parties. Some of them have been in existence for many, many years as you might imagine.

One of the questions that comes up is what do you do about those? Some of them are obviously with legitimate users so you don't have to worry that the bad people will register them or try to use them. Some of the domains you don't know whether they are owned by a bad person or not. You simply don't know because you can look in the WhoIs and you - so you don't know whether that's truthful who has information or not for example.

Man: But Greg can I stop you for a second? Because I don't understand this at all. But my under - I thought that the software tried to register those names. So if it's already registered, it simply will move on to the next one on the list, right.

Greg Aaron: No. No, the malware does not register the domain names.

Man: Okay, so what exactly is happening with the list of names?

Greg Aaron: Okay, it - the malware each day attempts to connect to a pre-designated list of domain names. And if it goes to that domain name

and finds valid instructions, then the botnet might do something or the (nodes) might get new instructions.

Now what happens is the bad guys know which domains those are going to be and then they will go out and register one or more of them for their use. So again, these are names that are potentially bad because the botnet can get instructions and then go do something bad to somebody, but they may or may not - those domains may or may not exist. They have to be registered and used to be efficacious.

Man: But they could put anything on their list. They could put Yahoo!, eBay, and everybody on their list then.

Greg Aaron: That wouldn't be useful because the domain to be used has to be controlled by the bad guys.

Man: No I understand, but still it creates the problem we have though.

Greg Aaron: Well they...

Man: Some of these names could be legitimately used by others.

Greg Aaron: Yes and in fact, that is the case. Again, some of these - there’s an algorithm that generates domain names. Most of them (gibberish), but some of them are short names and they are already registered and in use by people. In fact, some of them have been registered for many years by legitimate registrants. So you've got this issue of some of the names are an easier (cull) than others to put it another way.

George Kirikos: It's probably done intentionally to make it harder for the researchers also to throw you know 1000 good domains and one (gibberish) name. Researchers have a lot more work to do.

Greg Aaron: Yeah, (Andy).

(Andrew Steinglazer): So the - perhaps one of the missing elements on the chart is what we actually expect to have as actions. I mean so a whole bunch of these things are abuse, but defining them as such without sort of what we want to do about it doesn't get us very far, right. So sure a whole bunch of these pre-registrations - we know there's going to be harm if those things get registered and the bot tries to connect with.

And the next step is we want to define something that (has happened), right. And so if they put good ones on their list, that in and of itself isn't abuse - no big deal. But for the ones that are out there that we know the botnet may try and contact, all right what we're looking for is some sort of action to occur - some governance action or something like that to be able to take place.

And so the definition is fine in so far as we can define what actions we want to take for that kind of abuse. And perhaps that happens across the board here where some of these may be you know notified and others may be a cause for immediate harm if they are not dealt with in the case of for example some of these botnet control channel hosts. So we - a differentiator here is what you want the action to be. And so this is potentially malicious or it is malicious that it's going to go do those. We want some preventative action to take place.

Greg Aaron: Well I see where you're going. It does bring up the question of what the scope of the working group is to do. And we are not at this point making policy recommendations - in other words, saying in this case this thing should be done. That might be a job for a follow on group.

We do have the ability to say we think this is a problem and it should be looked at as a policy development process, or not, or dealt with in some other fashion.

So I just wanted to lay that out there. Efficacy and what our recommendation should be is important. There are some things that we may or may not be able to do though within the scope of our group. That's all.

George.

George Kirikos: And what is also tricky is that some of these are interconnected so that as the previous speaker was saying that for example the malware - those domains for example. You might not want to block them or you might want to block them but subject them to higher standards like making sure that their WhoIs is accurate. Because if you know for example that the WhoIs is accurate, you'll say go ahead and let the bad guys register them because that's a way to solve the crime.

Because you know you will have a map to their headquarters. But - and so that shows that they are interconnected because (unintelligible) WhoIs. If everybody had verified WhoIs, you wouldn't care about malware, botnet control. It's basically a map to their location.

Greg Aaron: I hear - oops, thank you for muting. Martin.

Martin Sutton: Sorry, but I'm - you know I was just thinking about that first definition there for the malware/botnet controllers. We're talking about more of intelligence gathering. From what we've - what security vendors, what law enforcement is finding out, and then acting on that in a proactive manner.

So I think we've seen instances lately where that's actually started to come through on the Conficker case. So I'm just wondering whether there is a better way of capturing that within that type rather than strictly down to malware/botnet control. This is where information has been identified, which could curtail abuse through potential policies that are adopted by registries and registrars in this particular case.

Greg Aaron: And so would you - I found the core of this particular item to be the pre-designation of domain names. Would you keep that or would you replace it with something to do with intelligence gathering?

Martin Sutton: I'd be inclined to replace it mainly because pre-designation - intelligence would mean you found something which means that something that is likely to be registered will have a fraudulent use.

Greg Aaron: Okay.

Martin Sutton: Does that make sense?

Greg Aaron: Comments anyone. Actually, I'm wondering if we should save that for next time.

Martin Sutton: Okay.

Greg Aaron: Because we have come up at the end of the hour. Marika has reminded me of an important thing. We are on a bi-weekly schedule. Two weeks from today is Easter Monday. That's a public holiday in some countries, especially in Europe. And I'm wondering if some of you may be off that day and whether we should reschedule that meeting. One option is to have our meeting as scheduled two weeks from today. Another option would be to have a make up meeting next Monday. Are there any preferences?

Man: Well first of all is anybody - two weeks from now, is that a holiday for people that are on the call?

Martin Sutton: Yeah, for me it is. Should we raise our hands?

Greg Aaron: Yes, if it's a holiday for you, could you raise your hand? Thank you. So far I see Martin.

Martin Sutton: Is that - sorry. What day are we talking about here then? Sorry.

Greg Aaron: April 6.

Martin Sutton: Oh, sorry.

Man: No, the 13th.

Greg Aaron: I'm sorry, April 6 is next Monday, and then the 13th is Easter Monday.

Martin Sutton: It is. Yeah, I will be away then as well. But that's a holiday - bank holiday over here.

Greg Aaron: Okay, is anyone else off on Easter Monday? Marika is off.

Marika Konings: But we can cover it internally. So you know if people want to have the call, Margie can cover it for me. That's no problem.

Greg Aaron: Okay, is anybody else off on Easter Monday? Okay, so far I only see two, which makes me inclined to keep it at the normal meeting time, which would be on the 13th. Martin is that a terrible inconvenience for you if we go ahead?

Martin Sutton: No, I probably won't be able to call in though because I think I will be traveling on the Monday, so apologies for that. But obviously if there is any stuff going to and fro between the next couple of weeks, then I can chip in.

Greg Aaron: Okay and of course we will record the meeting and we can bring you up to date offline.

Martin Sutton: Okay.

Greg Aaron: So I'd like to wind the meeting down then. Our next meeting will be on April 13 and I'd like to thank everybody for that document. It was very useful to have in front of us. Thank you for creating it and posting that up for our use.

Between now and our next meeting, Marika is going to circulate some revised definitions of abuse. And I'd encourage everybody to have a lively discussion about that on the list where we can trade comments and revisions. We'll also start revising the document that we put around today. We will add columns for additional notes and such, and we will continue to discuss that as well.

So any other comments before we conclude? Okay, if not, why don't we wind down and see you on the list.

Man: Okay.

Greg Aaron: Okay.

Man: (Cheers) Greg.

Man: Thanks everyone.

Woman: Goodbye.

Woman: Bye everyone.

END