BARCELONA – How It Works: Understanding DNS Abuse
Saturday, October 20, 2018 – 10:30 to 12:00 CEST
ICANN63 | Barcelona, Spain

UNIDENTIFIED MALE: Good morning, everybody. We'll start in a few minutes here, just waiting for a couple more individuals to show up. So thank you.

CATHY PETERSEN: Good morning, everyone. We will be starting very shortly. Thank you. Good morning, everyone. Welcome to our second session of How it Works today. For this session, we will be talking about understanding DNS abuse. Our presenter is Bryan Schilling, Consumer Safeguards Director at ICANN. I am Cathy Petersen, manager of the Office of the CTO. Welcome again. And we're ready to start.

BRYAN SCHILLING: Thank you, Cathy. As Cathy mentioned, I'm the Consumer Safeguards Director for ICANN, which is a new role to the organization. It came about – started last yes ear, but it came about largely through community interest in having ICANN start to talk a bit more about domain name system abuse.

In terms of how it works, we will go over that today, but domain name system abuse – or DNS abuse – is really something that ideally, we don't want to work, and the Office of the Chief Technology Office works to address some of these issues from a technical perspective.

I really would welcome questions at any time. I welcome this to be a very interactive discussion. I'm still learning a lot on the technical side of things when we talk about certain types of issues, so if there are those in the room who have information to add about some of the attacks that we'll go over, I welcome that, or any questions at any point in time. And also, I'll try to do my best at monitoring any online questions that come in.

So today, we're going to cover these four topics. That is, what is DNS abuse versus DNS misuse, we'll kind of talk about how we distinguish between those tow terms. We'll give some examples of both of those areas, we'll talk a bit about some of the evolving threats out there. There's some who say that the sky is falling. We'll try not to be that much of a pessimist, but – and then last, we'll talk about abuse within the context of ICANN.

Currently, there is no real accepted definition of what constitutes DNS abuse or misuse. It can encompass a number of areas such as cybercrime or cyber-enabled crime, such as hacking, malicious conduct. We'll talk about malware, botnets. In the context of ICANN, there's some in the community where we talk about it going further to encompass infringing material, copyright infringement, trademark infringement, but this presentation will primarily focus on the domain name system itself.

So, as we talk about abuse versus misuse, we've categorized this into abuse being focused on attacks or harmful activity aimed at the domain name system itself, versus misuse, which is more along the lines of

using the process that's in place for a person who would go about to use the DNS for nonharmful purposes to misuse it for harmful purposes.

So in this example here, someone who might be planning a malware attack, which would be an attack on the DNS itself, might use the registrant process and register multiple domain names under false identifying information. So it would be a process of misusing what's available to others for the intent of abusing the DNS system itself.

The DNS is such a vulnerable topic because it is vital to so many things. It's vital to individuals reaching websites, e-mails being delivered, devices being connected to each other. And it's so vital that if the system is disrupted, we know it can disrupt multiple trillions of dollars of ecommerce, as we're seeing a lot in the news more so these days, influence elections, disrupt communication networks. A number of things can be done through misusing or abusing the DNS.

So all elements of the domain name system from the authoritative nameservers to the recursive servers and stub resolvers are all vulnerable to various elements of DNS attack. As we can see here with this chart, the various types of abuse can impact all of these elements from bandwidth to the software that operates the servers to the various configurations as well as the cache, which we'll go into a little bit further in terms of how that can be corrupted in various aspects of the domain name system.

So now we'll get into some of these specific examples of the types of attacks that can occur and the types of misuse that can occur. Some of the specific abusive attacks cover a number of areas, from dedicated

denial of service attacks – and there are a couple there that we'll go into such as reflection and amplification attacks – to cache poisoning, and certainly other types of attacks that we'll take a quick look at.

So, DDoS, dedicated denial of service attacks, are a type of attack aimed at essentially crashing the targeted server for an entity. The attacker does this by spoofing their identity, launching multiple queries through the recursive and authoritative nameservers, and then sending larger packets of data so that this is all then gets aimed at the targeted server, and delivering, potentially taking that offline.

This is another type of, again, a resource dedicated denial of service where multiple messages and packets of data are being sent, essentially overloading the system.

Now, there are defenses to DDoS attacks that can be implemented within individual networks and servers, but the larger, better coverage for these types of attacks is more of an upstream filtering and defensive service, [up at your] higher network level or through the ISP level. Ideally outside of one's own network.

So, poisoning the cache is – excuse me. Cache is at different points in the query system process, a history is placed on various servers or within own individual devices so that when a query is made, it happens much faster.

In poisoning here, this one is an example of a spam attack where someone would click on the "lose weight fast now," which would go to an intended server and send back false information to the cache that,

in this hypothetical or in this situation here, would serve false eBay IP information so that it would then turn into a phishing attack whereby people would go to a different eBay.com server at a different IP address than the authentic, official eBay site. But that would all be done through the initial spam attack which would send back the false information to the cache.

Here again, we're offering some solutions and suggestions for how might defend against some of the cache poisoning. Certainly, as we see, keeping software up to date is vital on all elements of the network, and certainly, using DNSSEC as well will help potentially mitigate these types of attacks. And the link here on this slide will provide further information in that example on DNSSEC.

So, poisoning a host, again, is another type of attack where the – so we're missing some graphics on this, but in this situation, it's more of a piece of harmful software that's embedded on an individual device, like often from a spam or some other phishing and malware that goes on the device. And instead of it immediately redirects and individual to a false IP that then reroutes all queries to the DNS to their own intended targets and destinations of their choosing.

So here again, this is a bit more about keeping networks secure and patching software, ensuring that individual devices on a network are kept up to date. And certainly, as many of us are probably encountering taking opsec, operational security awareness training, probably a number of individuals are often caught perhaps by a test phish e-mail message that you might click on. So ensuring everyone is kept well

educated and informed about the types of attacks that are occurring out there is one good way to help protect and keep your network safe.

As we talked about, these previous instances were more about specific abuse and attacks on the DNS itself, the various servers, the authoritative nameservers, recursive servers and the whole query process and misdirection process. Next, we'll move into areas of misusing the DNS.

Registrations, as I mentioned very early on, are a ripe area for – sorry, missing another graphic here. But registering domain names is a ripe area for this in terms of being able to do this rapidly through different types of algorithms now to register multiple domain names in a very short period of time. It's often used or done with false information so that the registrant is masking their true identity, and so it's a potential corruption of various TLDs, the WHOIS system, and as well impacts various payment information.

And for those of you who've ever registered a domain itself, you know it's a very quick and rapid process that facilitates having active registered domains within a short period of time. And there are – while there's no direct link, there's some correlation and some potential circumstantial evidence that very inexpensive registrations can lead to high instances of abuse within certain TLDs.

So, here are some of the reasons why some individuals might decide to falsely register domains. First of all, the domains can be used to set up phishing sites, are used for distributing and receiving and redirecting types of malware and botnets. They're used for those command and

control scenarios. And also, they might be engaging in actual illegal or ecommerce such as selling illegal pharmaceuticals, potentially selling infringing material. So there are a number of reasons why individuals might want to register a domain for nefarious purposes.

Another type of misuse is an actual hijacking of legitimate domains or legitimate registrant data. This could be used for all of the various types of activities that we've already talked about, such as distribution of Malware, taking over or establishing a command and control for a botnet, but what this is then doing is it's being done on somebody else's domain who registered that domain and is using that domain for legitimate and perhaps ecommerce purposes.

Another aspect of this slide – we're missing some visuals on here, some graphics, but one of the things that is also a concern is the number of data breaches that have occurred out there. For example, we know with Yahoo that there were e-mail addresses and passwords. So there's a number of resources and information of available for individuals to take somebody else's identity and be registering domains as a result of the numerous data breaches. And that's something that we know is out there but we don't necessarily have a direct correlation to that yet.

So, in this area of misuse and ways to prevent this, certainly using registrars that have two-factor authentication with their registrants and our putting in more operational security features to validate that registrants are the actual – that the people behind the domain can be identified, known and contacted is a good thing to work on from a

registrar perspective, and from a registry, is to engage in work in registrars who offer these types of operational security features.

Fast flux is another type of abuse that is certainly debated and is talked about. There are legit uses for fast flux in terms of this is setting the time to live on the movement of various IP addresses, and there can be certainly legit reasons to have redirecting at various levels.

But those engaged in abusive activity are setting that very rapidly and abusing it such that to detect where perhaps a malware is being sent from or data exfiltration is being sent to keeps moving at such a fast pace that it's hard to track and identify the individual behind a malware or botnet attack. So it's a defensive tactic used by those who are engaged in abusive activity to try to thwart any law enforcement or security investigations.

Bear with me here while we get through a couple slides that are missing some graphics.

UNIDENTIFIED MALE: [Are these slides going to be available?]

BRYAN SCHILLING: Yes.

CATHY PETERSEN: Yeah.

BRYAN SCHILLING: With the graphics. So, with certain malware and botnet attacks, the intent is to penetrate a network and pull out certain data, perhaps proprietary or sensitive data from a company, credit card information, banking information, and these types of attacks, coming back with the fast flux thing, can be hard to track. But some of the more recent types of attacks that we've seen, such as the ransomware, which we'll talk a little bit more, which have been more about freezing a network, holding data, information for a ransom is connected to this, but the botnets tend to be more extensive, and sometimes, tracking where that information is going is vital to solving some of these issues.

Now I'll move into some of the more evolution types of threats. I had just mentioned ransomware, but here, DDoS has been around for a while. There are actually entities where – we'll call them stressers, so you can go and buy a DDoS attack, and it could be marketed as for security officials to stress a system, to test things, but it can also be purchased for nefarious reasons.

We'll also talk a little bit more about the Internet of Things, which some in OCTO will call the Internet of Threats because of the large number of devices now connecting to the Internet and the vulnerabilities that are within the actual hardware itself. We've seen a lot of that in the news recently with various companies distributing routers that have set identifiers and passwords.

So these are a couple, as I just mentioned, aspects of readily available types of tools for initiating DNS abuse such as the stressers, the DDoS

attacks. All of these are out there that can be purchased or utilized and are cloud-based services.

Avalanche was a large malware network that was disrupted a couple of years ago by a global law enforcement effort. It was a botnet that was distributing malware and was predominantly used for financial fraud attacks. But down at the bottom of this slide, you can see there were a number of types of malware that were used in the overall avalanche investigation and overall attack.

And this was a large-scale developing malware and evolving malware attack that took place over almost eight years from the point of time where the initial malware was evolving in 2008 into 2009, and as you can see here, it evolved here into a larger botnet delivery system in 2010 to 2012 timeframe.

And then from 2012 to 2016, a number of law enforcement, security entities, private companies were involved in a takedown of this Avalanche investigation that impacted 64 TLDs. Yeah, there were multiple operations in multiple countries.

Unfortunately, we're missing a graphic here, but – under attackers operate at Internet pace. This is kind of – if you could imagine a timeline on this slide where there's a comparison of how quickly an attack can happen versus how quickly somebody can ultimately be detected and arrested, an attacker is going to be developing their malicious code, and they'll launch that malicious code, and within hours, it will have an impact on victim networks and victim computers.

Generally, the first to detect that is going to be the private sector who's monitoring their large networks. Once they detect this attack, or security researchers – we'll get to here, there's some really interesting – talk about timeline about some of the security researchers, how quickly they moved, how they function with exchanging information through Tweeting about it and that, and being able to respond.

But then, this timeline shifts, it slows down very much, because then you move into the law enforcement and government investigation phase, which, to get to the point of where you're actually putting handcuffs on somebody, removing somebody from behind a keyboard, can take months, if not years through the mutual legal assistance process, through police to police cooperation, and in a manner to gather evidence that can be used to actually prosecute someone.

CATHY PETERSEN: Let me try to upload a different format.

BRYAN SCHILLING: Okay. Alright. We're going to try to modify this slide here. But you can just imagine that when a person initiates attack, their harm is created within hours, versus the months and years it can take for law enforcement to respond to that. Give it a second here.

Are there any questions or any points while we're waiting for slides to be adjusted? Hopefully, we can get to a slide where ewe talk a bit about the impact that Avalanche had. I recall that around 40 to 60 different TLDs were impacted, around 830,000 domains were impacted, there

were arrests in multiple countries, somewhere – talk about I think multiple, if not over 100 servers were taken offline across the globe in response to the Avalanche attack.

CATHY PETERSEN: [This is taking a while.]

BRYAN SCHILLING: Bear with us for a minute here, please.

CATHY PETERSEN: You were on slide 30 –

BRYAN SCHILLING: 32.

CATHY PETERSEN: Yeah. Okay.

BRYAN SCHILLING: Or, yeah, we can go to 30.

CATHY PETERSEN: Yeah, you can use this right now.

BRYAN SCHILLING: Okay. So yeah, on the Avalanche outcome, I've got it pulled up here. We had five arrests in four different countries, there were 37 searches in seven countries. This would have been law enforcement searches and raids. 39 servers were seized in 13 countries, 221 servers were taken offline. I was way under there. 64 TLDs, and 830,000 domains in 26 countries were impacted. And then it moved into identifying victims and seeking remediation.

Oh, great. Okay. That was the slide we were on. Thanks, Cathy. I'll just back up here. Oh, can you go back? This one, yeah.

CATHY PETERSEN: That one is not working.

BRYAN SCHILLING: First day troubles for ICANN meeting.

CATHY PETERSEN: It's not this one, right?

BRYAN SCHILLING: No.

CATHY PETERSEN: Sorry, it's Adobe.

BRYAN SCHILLING: Okay. That's okay.

CATHY PETERSEN: The Adobe is – it's working –

BRYAN SCHILLING: Yes. Okay, it's working in the – okay, sorry. So that's the timeline for those who are in the Adobe Connect room. We moved on to the outcome, which are the bubbles. But then –

CATHY PETERSEN: It's really weird. [inaudible]

BRYAN SCHILLING: [inaudible]. No.

CATHY PETERSEN: Try the clicker. Want to try the clicker?

BRYAN SCHILLING: Sure. Okay. Despite the extensive involvement in the Avalanche outcome, there was, again, another evolution of malware called Andromeda that was a follow-up to Avalanche. Avalanche was disrupted in late November 2016. Andromeda came out after that and was disrupted about a year ago in December of 2017.

And it too was – there's a link on the slide here that's to a press release from Europol about the extensive cooperation between Europol, the

FBI, Microsoft, and others that were involved in dismantling the Andromeda malware.

Mirai, as we talked about a little bit earlier, the Internet of Things or the Internet of Threats, Mirai is a type of malware that is aimed at attacking vulnerabilities in the hardware that is now connected to the Internet. And it's primarily aimed at Internet routers that are shipped with manufacturer identifying information and known passwords.

It's a malware that takes advantage of all of us who don't go in and change that standard information that comes with a device, so the fact that we're plugging routers or other devices into the network and not going in and updating or changing security features. So it's constantly scanning and looking across the network for those largely open devices, and then utilizing those opportunities to distribute malware further.

In 2016, there was a large – this malware was known for, there was a large article about a particular corporation, Dyn Corp that was essentially knocked out because of all the open vulnerabilities within their routers.

And this isn't just a large network, this goes into all of our individual homes and devices that we are now connecting to the Internet. So here, kind of a diagram, and as you can see on the left side of the screen, some of the points here that this was just scanning for hardcoded vulnerable information that isn't being changed in the devices themselves.

In terms of being able to mitigate this, network operators need to ensure that any hardware is being modified so that the Mirai virus cannot go out and scan for known manufacturer IDs, and these devices, once they have been corrupted, as indicated here, are being then repurposed or being used to go further into a network and distribute malware or potentially data exfiltration.

So WannaCry, WannaCrypt is the ransomware that has been in the news a bit more these past few years. There was the large attack recently that hit the National Health Service in the UK and a number of other organizations.

This was a ransomware that would go in, secure the devices and was seeking payment in Bitcoin. What was interesting about WannaCry and WannaCrypt is that it was – there's some debate whether the person who created it made a mistake or was intentionally trying to keep his malware out of a sandbox.

A sandbox is where security researchers and law enforcement will study malware to try to hopefully break it down in a safe and secure environment and try to attempt to figure out what's going on. In the instance of WannaCry, a security researcher identified that the malware was constantly going to an unregistered domain.

So this researcher went in and quickly registered the domain, and as a result, ended up killing the distribution of the malware. And the thought here was that the individual who created WannaCry wanted to keep his or her malware out of a sandbox, didn't want security researchers to be able to break it down, and so as the malware and ransomware was

pinging the unregistered domain, it was searching for common IP addresses to see if it could know that it was in a sandbox.

So the sandbox would have been sending the same IP address. And once that started happening, the malware was designed to shut itself down. And so the WannaCry ransom was essentially killed by a potential fault in the malware itself or it perhaps was intended to be that way. But it was one that was fortunately ended fairly quickly because of the security researching community out there who responds to these types of attacks very quickly, is analyzing information and sharing information and figuring it out.

So, abuse in the ICANN context. Abuse in our context is a bit of a different area for discussion in the community. Within our bylaws, we are tasked with responsibility for maintaining the security and stability of the Internet.

So types of DNS attacks that go right to the heart of the system, such as the DDoS attacks that were mentioned, some of the malware attacks aimed at the authoritative nameservers, the recursive servers, those are abuse that ICANN is involved with, will work with individuals, work with networks to help secure them, will provide information to law enforcement to help them understand how the networks work so that they can respond to these types of investigations.

But then we have some to her types of abuse that are a bit more controversial within the community. One such area is spam. Our bylaws also restrict ICANN from doing anything that would be about regulating content, and there's some discussion, is spam protected content, or is

it largely a type of abuse that can be used as a vector for larger forms of abuse such as malware distribution, phishing, other areas?

Certainly, some of our current hot topics, as we all know, is WHOIS and GDPR and having law enforcement and security researchers and others have the ability to gain access to WHOIS information so that they can identify individuals or identify the trends in misusing registrants and domains as we talked about how that can be done in effort to then go further in DNS abuse.

So, in terms of reporting – well, let me start here with the Governmental Advisory Committee and the Public Safety Working Group. During 2013 and subsequently in 2016, the GAC issued these two provisions within their communique about ICANN needing and the community to discuss whether ICANN should be more involved in mitigating abusive activity within the DNS.

You can see here in the 2016 that the GAC conveyed some areas that were of concern and that ICANN should – the community should look at, and there you can also see where we talked about spam and the debate that continues in respect to, is spam a type of abusive activity, or is it protected content?

So, within the Governmental Advisory Committee, there is the Public Safety Working Group, which is primarily made up of aspects – governmental entities that are involved in protecting consumers such as law enforcement, but it goes further with various types of entities that are in various countries that are about protecting privacy, protecting consumers from harm, protecting some of the

pharmaceutical, illegal pharmacy issues. So it's broad. It does not just include law enforcement entities.

And as we mentioned earlier, one of the hot topics within the Public Safety Working Group is some of the fast flux issues, which again is the rapidly changing of IP addresses so that malware is hard to track or data exfiltration is hard to track.

There are some areas for abuse to be addressed within our current contracts with registries and registrars. As many of you know, registries and registrars are required to respond to abuse complaints. Now, that can take a number of forms.

It could mean that if they investigate something, they're unable to determine that a particular domain name is actually engaging in abusive activity, it could also mean that legal demands would be necessary to respond to that, such as a court order or a law enforcement demand.

But there are elements within the existing ICANN contracts and environment for contracted parties to address abuse and respond according to their agreements.

With that, [I'll] happily open up to any questions or comments or anything. But thank you for everyone's time, and thank you for bearing with us through the missing graphics. But I think we have it fixed now, and the slides will be available for the pictures.

CATHY PETERSEN: I'll also be reading out questions from the chat room. In the meantime, just a reminder, please state your name and affiliation. Thank you.

BRIAN CIMBOLIC: Hi. I'm Brian Cimbolic, I'm with Public Interest Registry. I just have a question, Bryan. You mentioned about spam being a vehicle for delivery of other types of abuse, which hi totally get and agree with, but I was wondering if there's any data as to what percentage of spam sent on a daily basis actually contains separate DNS abuse. Is it the majority, is it a significant percentage? Do you have any hard data on what – I don't mean to put you on the spot, just curious.

BRYAN SCHILLING: I'm on the spot, but thanks, Brian. I'll look into that and follow up. I think that's part of the issue. There are a number of reputation block lists out there that are monitoring spam, and that is being used by the various networks. But I don't have the specific numbers on that. But I'll certainly follow up and see if we can –

BRIAN CIMBOLIC: Yeah, fair enough. If you could just point me in the right direction.

BRYAN SCHILLING: Absolutely.

BRIAN CIMBOLIC: Alright. Cheers, Bryan.

BRYAN SCHILLING: Thanks, Brian.

MICHELE NEYLON: Good morning. Michele Neylon from Black Knight. I'm really worried about the scope creep. You guys are going off down into little – down rabbit holes where you should not be going. Issues like spam are completely outside your scope. Completely. If you want to address spam, you need to address it elsewhere. It is not something that ICANN should be getting involved with.

And your commentary around WHOIS, I find really offensive. As a senior ICANN staffer, it is not you who dictates policy. It is those of us who are trying to comply with the law, and those of us who are working within the policy. In other words, this kind of posturing around how WHOIS could or should be used is really offensive. Thank you.

BRYAN SCHILLING: Thank you, Michele. I think your comment on the scope is certainly something for the community to be discussing, and that was part of the role of the consumer safeguards department, was to come in and have these discussions and have it be a cross-community discussion so that we could narrow down that question as whether or not it is within our scope or not within our scope. So I welcome that discussion, it's something I would like to – hope that the community would find some time to address that so that we can kind of either – figure out where that direction is going.

MICHELE NEYLON: No. That's like saying, "Okay, let's create a department to fix an issue that we've decided is within scope. Now we've got the department, we're now going to ask you, is it within scope?" That's completely ass backwards. You can't go off, build a department to cover something which isn't in scope, and then ask, "Is it in scope?" That's backwards. That's completely backwards.

I mean, it's very ICANN-esque and it shouldn't really surprise me, but it is completely backwards. I mean, there are many issues that ICANN should probably deal with, there are dysfunctional entities out there that need to be addressed, but trying to give yourselves more things that are outside of your scope and remit is nuts. It's absolutely nuts.

I mean, ICANN is meant to coordinate the technical identifying resources. It is not some kind of global Internet police or something. I don't even know what you're trying to frame yourselves as. But to kind of look at it in that – the way you're presenting it is completely illogical.

BRYAN SCHILLING: Okay. Thank you for those comments, Michele.

DEAN MARKS: Hi. Dean Marks. For those of you who know me, it may come as no surprise that I just wanted to state a different view from Michele's view, which is that, I think, as part of ICANN's bylaws and charter, there's a responsibility for the security and stability of the DNS infrastructure.

So to the extent that abuse that you described and misuse destabilize the DNS structure, I think it's well within ICANN's remit, whether it addresses WHOIS or any other element of the DNS system. So, I for one appreciate the efforts that the CTO team and the Compliance team are doing in this respect. And my question is, where will the slides be available? Are they – I mean, where will we find them? Sorry. Thanks.

CATHY PETERSEN: The complete slides are already uploaded in the public schedule.

DEAN MARKS: In the public schedule.

CATHY PETERSEN: Yes, and the graphics are all there. For some reason, the Adobe room was – we're having issues with the Adobe room, but the complete slides are –

DEAN MARKS: So we can just go to the schedule and find them.

CATHY PETERSEN: You can go to the public schedule for this session, and the slides are already there.

DEAN MARKS: Thank you.

CATHY PETERSEN: The recordings for this session and the transcripts will be published also to the public schedule within a week or two.

DEAN MARKS: Thank you so much.

CATHY PETERSEN: I have somebody in the remote room. He has some comments and questions, and I'll just read it out before you. Thank you. From Farell Folly, he would like to know more about the security of Internet of Things within ICANN, and is there any PDP WG planned to be set up, any advisory committee to discuss that? He also said that the presenter, Bryan, discussed how Internet of Things could change the security and privacy aspects of the Internet, and it seems to be the new waves of threat. Otherwise, what is ICANN's plan?

BRYAN SCHILLING: Yes, Farell. We'll have to respond back to that specific question. To clarify that IoT could change the security and privacy aspects, I think it's already impacting the security and stability when devices are being penetrated and exposed because of weak security aspects, and then seeing as we saw with networks just being completely taken out because of those vulnerabilities.

And certainly, there's evidence of data breaches and private information and financial information being exfiltrated from

vulnerabilities in the devices themselves, but I'm not aware of a PDP or working group on this issue yet. I think there might be some discussions in the SSAC area, but we'll have to follow up on that specifically.

AJAY DATA: Ajay Data from India for records. I always wondered the number of spams. I really don't care whether in scope or not. I'm interested to know how do you – DNS abuse happens every day, every second, and the spams are increasing every last ten decades I am seeing – ten years. And there is no way that somebody at a community level is probably dealing with it within ICANN.

So I have two questions. One, where do you set up a group or where do you go to deal with this and discuss it more further to have a concrete solution to avoid a DNS abuse? At least for spam, one. And secondly, is there any mechanism where somebody is found guilty or somebody's network has forcibly used for commercial gains, is there any mechanism to take this network off the Internet? Thank you.

BRYAN SCHILLING: Thank you, Ajay. In terms of the first part of the – to have a discussion around spam needs to come from within the community. And whether it comes from one of the advisory groups, the SO/ACs, so coming up from that and to address that topic, it seems like there could be a potential for that as we've already heard from two community members with opposing thoughts on it.

In terms of your second question, I'm not aware of specific entire networks being taken out just for spam. I know there are a number of reputation block lists that monitor traffic for spam activity and provide that information to network providers that goes into our browser information that helps block that and filter it out and keep that. But I'm not aware of any specific law enforcement or other action that was aimed wholly at spam.

And in spam itself, a lot of it sometimes is not what we see show up in our particular e-mail, but then also some of the information embedded and the content of that itself is some of the – like the example we gave earlier on the "lose weight fast now" and how that link was then used to redirect and change IP information for a legitimate site.

But thank you for those questions, and I can look into certainly the actual – if there's been a network taken off just for spam purposes.

CATHY PETERSEN: I have another question from a remote participant, Suhay. Can ICANN block any website that sells DNS DDoS attacks?

BRYAN SCHILLING: ICANN itself does not block or suspend domain names or websites. That would be something that the actual registry or registrar would need to take action on. So that falls within reporting that abuse to the particular registry or registrar and/or law enforcement entities or others that would be involved in that. But ICANN itself does not go in and suspend domains for items like that.

UNIDENTIFIED MALE: Thank you. Because from the last two slide, I think you show us about the Public Safety Working Group. So I was wondering, in particular with law enforcement, because from the first slide, you show us about what happened with – how DNS abuse lead to many crimes, many cybercrimes which are related with the commerce activity.

So I was wondering what has been done between ICANN, maybe with another, law enforcement maybe for example, maybe with Interpol, how to tackle the issue for example. I think it's already been said by the other participant about the spam, but maybe also there are other things here, because the lack of harmonization, but nature of the cybercrime itself is borderless. So, are there anything that maybe has been done or something, because I still quite new, and it's the first time I'm attending ICANN event. Thank you.

BRYAN SCHILLING: Thank you. Hopefully, I understand in terms of what's being done to address cybercrime, which is largely borderless. Primarily through law enforcement cooperation and security researchers, and private entities who are detecting various abuse and threats and reporting that, sharing information to address it. Europol is heavily involved. With Interpol, there are computer emergency response teams or CERT teams across the globe, and that network is sharing information and working together.

From an ICANN perspective, we will share our information about the network, and we'll sometimes train law enforcement so that they understand how the DNS works so their investigations can function in a way that doesn't harm the network itself. You know, sometimes suspending or taking servers offline or other things can have a more harmful effect potentially than resolving the criminal activity itself.

But I know there's a number of individuals in the Public Safety Working Group that would be able to shed more light on how law enforcement organizations are cooperating in this space and sharing information, whether that's through Interpol or Europol or the various different national organizations.

JANOS SZURDI: Hello. I'm Janos Szurdi, PhD student and newcomer fellow, and my question is related to the part where you talked about abusive domain registrations and domain hijacking, and the possible defenses that were all some kind of passive prevention approaches such as two-factor authentication or DNSSEC.

My question is towards more active approaches and active detection, and what thought has been put into this. And a good example could be any big and advanced tech companies whose main defense is not that they require you to have phone or an e-mail address or such measures, but they build sophisticated models to detect account takeovers, which is the counterpart of domain hijacking or fake accounts, which is the counterpart of hijacking domains. No, that's the abusive domain registrations. Sorry, I got confused here. But – so the question is, what

steps are taken in this regard, and is this something that is considered, and is there a potential for collaboration in the ICANN community? Because that would be probably the most powerful way to get rid of all this abusive registration, domain hijacking.

BRYAN SCHILLING: Thank you, Janos. Welcome to ICANN, and it's great to have you here. First, collaboration is across the community, and certainly, having those discussions and ideas is a way to share ideas and practices. There are some that would suggest that a registrant's domain isn't readily available for use, that there's actually a little bit of a lag in time for there to be verification of the person's identity.

There's some filtering aspects that can look at some of the registration information and alert that out there. The registrars vary in size and operational activity and across the globe, so there's various levels of processes and applications and features that go into actually how a registrant information gets shared or verified and matched with payment information.

So I think there's a lot that can be done and discussed to improve that area, whether it is the two-factor authentication – in terms of the hacking, I think that also – there's other groups there that are working on those issues too.

We don't seem to have any more questions online. If there's not any here, I appreciate everyone attending, and –

CATHY PETERSEN: Oh, we have one more.

BRYAN SCHILLING: Oh, we've got one more. Okay.

AJAY DATA: [inaudible]. This was going on in my mind. I thought, should I ask or not? Do we also address dark web somewhere in DNS abuse? And how do we tackle that?

BRYAN SCHILLING: The dot web?

AJAY DATA: Yeah.

BRYAN SCHILLING: Oh, the dark web, sorry. I think that's a much broader question too. I think we're focused on – kind of back to Michele's point right now about looking at matching the technical identifiers and where are the things within the domain name system that are within our responsibility of maintaining that security and stability.

I think there's certainly discussions being had about the dark web within the Public Safety Working Group and others, but what we're focused on or talking about right now are those types of abusive activity

that are occurring at – targeted at the domain name system or that are misusing the DNS to engage in abusive activity.

UNIDENTIFIED FEMALE: Hi. Thanks for your time. What's the view of ICANN about Conficker worm? Do you remember Conficker worm? [inaudible] a number of years before.

BRYAN SCHILLING: Sorry, what was the question about the worm?

CATHY PETERSEN: Conficker.

BRYAN SCHILLING: Yeah.

UNIDENTIFIED FEMALE: Well, what's your view about Conficker worm? Do you remember Conficker worm? Yes. Yeah.

BRYAN SCHILLING: I think certainly, the Conficker worm was certainly a type of abusive attack that occurred. What we've seen more are some of the activities that we talked about today in terms of – that are aimed at the DNS, the DDoS, the malware distributions and others. But happy to talk offline a

bit more about the specifics there or get you in touch with some people who are a bit more experts on that particular attack than I am.

RUDOLPH DANIEL: Hi. My name is Rudy Daniel, I'm an ICANN fellow. Going back to spam, obviously, any abuse of the DNS system threatens the security and stability of the network. So, where does ICANN draw the line when it talks about content and controlling content? Which I know that we have an issue with.

BRYAN SCHILLING: Thank you, Rudy. Pursuant to our bylaws, we have no role in regulating content. And that, to your point is, as we've seen in respect to spam and some other areas that sometimes the community has discussions about, but it's outside of our remit as things stand.

RUDOLPH DANIEL: So, if I can come back to you then, so the argument about spam is that – what is the – should ICANN get involved in spam? We've had this from a couple of conversations before.

BRYAN SCHILLING: Thanks, Rudy. I think you're right, that is an argument. I think it's more of a conversation like if you look at the Spec 11 public interest commitments that are with the new TLDs, within that, off the top of my head, phishing is mentioned, malware, botnet, but spam is not in that category of a public interest commitment to address.

So if there were to be that discussion within the community and the community were to move towards potentially adding spam to that, that could happen. That's for the community to decide how that direction goes. But you're right, there's of two minds out there, and until we actually have the discussion about it, we won't be able to say for sure. But as it stands right now, anything with content, our bylaws prohibit ICANN from regulating. Which I think is –

RUDOLPH DANIEL: So therefore, there is a globally recognized definition of spam?

BRYAN SCHILLING: There's not, no.

RUDOLPH DANIEL: OKAY.

CATHY PETERSEN: One more.

MICHELE NEYLON: Just on that gentleman's point, I understand what he's getting at, but I think the reason that some people [don't] understand why people like me will push back so hard on this is because spam writ large is completely subjective. One man's spam is another man's marketing, like the one mean's freedom fighter is another man's terrorist, or the other way around.

Looking at phishing and actual abuse of the DNS, pure technical abuse, DDoS, distribution of malware, those kind of things, they're pretty objective. It's very hard for somebody to say a phish is not a phish. It's very hard to say a malware isn't malware, etc.

But when it comes to spam, trying to do it at the ICANN level is a horrible idea for a multitude of reasons. The registry operator has only got the ability to pull a domain, there is no way to pull part of a domain. As a registrar, I have the same problem, I can take an entire domain offline, I have no way to simply stop the e-mail. I have no way to simply stop one type of traffic. That is not how things work.

That doesn't mean that those of us in the infrastructure space don't want to mitigate this, but ICANN is not the place for that. If people need to have those conversations, they're happening elsewhere between the RIR space. RIPE has an anti-abuse working group, I'm sure ARIN has various different things, MAWG, APWG, there is a lot of other places. But you do not want ICANN getting involved. That'll be a terrible idea.

DEAN MARKS: So, I just wanted to say, Michele, that I feel what you just said now really sort of divides things in a more helpful way than – at least to me, your first remark, which I thought when you got upset, "No, ICANN shouldn't be involved in phishing and malware and denial of service attacks or other clearly illegal activity," I may have misunderstood.

And so what I wanted to say, just for the record, is I think spam is a complicated issue. I think Michele is correct that it's very difficult to

draw the lines between what's speech, what's spam. And so I had sort of thought that more of what you were talking about with spam was when the spam was sort of overwhelming the system and things like that. But again, I could have been wrong.

But I just – given the earlier discussion where it seemed like Michele and I were completely in disagreement on what ICANN was doing in this abuse space, I think based on his last remark and this remark, I think there's a lot of agreement that malware, phishing, botnets are clearly identifiable abuse, there can be illegal activity that's – whether it's copyright infringement or sale of counterfeit goods, Michele may disagree with this, but that's illegal activity that can be seen as abuse. And I do think spam is a little bit more of a gray area. So, for the sake of community, I feel like if there's movement towards more consensus, that's a good thing. Thank you.

BRYAN SCHILLING: Thank you, Michele and Dean. It is a gray area, and that's certainly why it's a topic within the community. As we gave the one example, the spam can be used to the manipulate the DNS where we gave the example of the loseweightnow.com example where that then – when that domain was then sending back to change redirection and cache information to – so it's that gray area, and whether it's within this community or it remains outside with the other individuals and experts who are looking at it too is certainly up to the community.

AJAY DATA: I think the session is becoming more of a spam than anything else. But it is great, because I deal with anti-spam applications, and my pitch is always, virus is virus for everyone, spam is not. And that is – we all will agree. But if not here, then where? It has to be discussed somewhere.

MICHELE NEYLON: [It is. It is discussed elsewhere.]

AJAY DATA: So, now the problem is – and we have been seeing that in last ten years, as I said, spams have only increased and spams have only increased. Probably, we need more platform, more discussion around that. I would love to know where it has been more discussed and we can participate. Ultimately, it has to stop somewhere, it has to be controlled somewhere.

What are the mechanism? I think we all will agree, nobody will disagree that we [need to do something] with that. We have to deal with that. And it is also very obvious that it is not for the spam. Spam is for not everyone. That is also true. But there has to be some mechanism where we can find the legitimate [sender or legitimate sender] and then control that. Thank you.

BRYAN SCHILLING: Thank you, Ajay.

UNIDENTIFIED MALE: Could you distinguish – clarify that [inaudible] [registrar] is part of Internet intermediaries? To clear my understanding, Internet intermediaries, because as Internet developed, the obligation for those who in the past maybe just opened infrastructure, now they also need to be responsible with the content itself, and then I think spam is only one of the example, but that's also happened in other places as well, in other platforms as well. So, do you think it's because the definition of the activity or the collision of different technologies creating another level of crimes, which makes the responsibility that maybe 10 years or 20 years ago maybe not, but now, people start to collision each other? [Same like] how the business model it works itself. Thank you.

BRYAN SCHILLING: I think – I'm understanding that [inaudible] there are criminal networks involved in cybercrime. As we illustrated a bit with the Avalanche takedown, that is the case, that there were a number of individuals arrested in multiple countries. We know that they work together. In the same way security researchers share information, other individuals share malware.

The Mirai malware itself was posted and was an open source malware that is still potentially out there. we've certainly seen groups who coordinated together and coordinated attacks together, as we illustrated with the Avalanche. So yes, I think there are networks out there engaged in that type of activity.

Okay, I think we're finished then. We didn't have anything online, so I appreciate anyone's questions and thoughts on topics to be further

discussed as well as your time here this morning, and hope the rest of your week at ICANN is as lively.

CATHY PETERSEN: Thank you, everyone. Just a quick reminder, our third How it Works tutorial today will be at 1:30, and we will be talking about Internet networking. The room will be changing. We will be at room 127. Again, it's room 127 at 1:30 for Internet networking. We will be talking about IPv4 and IPv6 and such. Thanks again.

And again, all the slide materials are already uploaded in the public schedule with the complete graphics. Recordings and transcripts will be posted within a week or so. Thank you.

MICHELE NEYLON: [inaudible]. You have no idea what we actually do, do you?

UNIDENTIFIED MALE: [inaudible]

MICHELE NEYLON: Yeah, that's true.

UNIDENTIFIED MALE: What do you mean? On the spam stuff, or on the –

[END OF TRANSCRIPTION]