ICANN69 | Virtual Annual General – DNS Abuse
Tuesday, October 20, 2020 - 10:30 to 12:00 CEST

SPEAKER: Test for our language services team.

Interpretation for the session will be conducted using both Zoom and the remote simultaneous interpretation platform operated by Congress Rental Network. Encouraged to download the Congress Rental Network app following instructions in the Zoom chat or from the meeting details document available on the meeting website page. If you wish to speak please raise your hand in the Zoom room and once the facilitator calls your name our technical support team will allow you to unmute your microphone. State your name for the record, if speaking a language other than English, please state the language you will be speaking. When speaking be sure to mute all other devices and applications including the Congress Rental Network application. Please also speak clearly, and at a reasonable pace to allow for accurate interpretation, this concludes the audio test.

Please advise if you would like me to read this again. Thank you.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

SPEAKER: Hello, and welcome everybody. We will be starting in just one minute. Thank you.

SPEAKER: The session will begin, please start recording.

OZAN SAHIN: Hello, and welcome to DNS abuse plenary session I'm Ozan Sahin, and I am the remote participation manager for the session. Please note the session is being recorded and follows the ICANN expected standards of behavior.

During the session questions or comments will only be read aloud if submitted in English within the Q and A pod. This feature can be accessed from the Zoom tool bar. I will read questions and comments aloud during the time set by the chair or moderator of the session.

This session includes realtime transcription and interpretation. To view the realtime transcription click on the closed caption button in the Zoom tool bar. Interpretation for the session which will include Arabic, Chinese, English, French, Russian, and Spanish and will be conducted using both Zoom and remote simultaneous interpretation platform operated by Congress Rental Network. Attendees are encouraged to download the

Congress Rental Network app following instructions in the Zoom chat or from the meeting details document available on the meeting website page.

If you wish to speak please raise your hand in the Zoom room and once the session facilitator calls upon your name our technical support team will allow you to unmute your microphone. Please state your name for the record and the language you will speak if speaking a language other than English. When speaking be sure to mute all other devices including the Congress Rental Network application, please also speak clearly, and at a reasonable pace to allow for accurate interpretation.

I would like to highlight that remote participants are not able to click on the microphone button and unmute themselves during the meeting without assistance from the technical support team. For all participants in the session you may make comments in the chat, to do so please use the drop down menu in the chat pod and select respond to all panelists and attendees to allow everybody to read your comment. Please note that private chats are only possible among panelists in the Zoom webinar format. A message sent by a standard attendee will be seen by the hosts. Co-hosts and other panelists. With that I will hand the floor over to Thomas Rickert. Thomas?

THOMAS RICKERT: Thank you very much, OZAN. And good morning good afternoon good evening everybody I am Thomas Rickert. I'm director names and numbers with economic satisfactory of the Internet industry which is actually one of the co-hosts of ICANN69 so I would like to welcome you virtually in my home country Germany. I'm in BONNE. I would have love to travel to Hamburg to see you in person but unfortunately, that is not possible this time around. I hope that we are going to have an opportunity to engage in the very near future and I hope that you are all safe. Let's please move to the next slide.

As OZAN mentioned already, this session is about DNS abuse, and actually in ICANN's history there have Bonn a lot of sessions and DNS abuse and I think the reason why this topic is keeping us busy is because actually there is a lot of bad stuff going on and off the Internet. A lot of bad actors are trying to exploit the lack of knowledge of users and try to lead them or mislead them to offerings that they shouldn't be going to, and cause financial and other damages. I think that for ICANN this topic is very special given ICANN's very limited mandate according to ICANN's bylaws, and that is why I guess it's important to continue the dialogue on DNS abuse, to understand what the issue is, to understand what the roles and responsibilities of the different players in the Internet ecosystem are and then also look at what the solutions or potential way forward could be.

Actually during the session I hope that we can do a little bit of all of the above, but we are trying to focus on solutions and ways forward. Today we're going to have a 90 minute session and the way we are going to conduct this is we're going to have presentations by speakers which I'm going to introduce to you in a moment, and then we're going to pause after each of these interventions briefly to see whether you have written any questions into the Q and A pod. So we are going to try to answer the questions that you can type in there, and please keep these questions to those that are actually related to the speaker that you just heard so in case there is something unclear in the presentation of the speaker we are trying to sort that out. But after the speakers we are going to have a Q and A session at the end of this 90 minute session and that's the opportunity for you to ask more general questions, and you can do that both in the Q and A pod as well as by raising your hand and then the technical folks will likely unmute your microphone and allow you to join the discussion, on the -- you know by making oral interventions as well. So my opening remarks and introductions are going to be over soon so we can try to talk about -- dive into the substantive cause in a few seconds. So just so that you know whom you're going to have some DNS abuse information exchange with today we are going to hear in David Conrad first and then we will hear in Jeff Bedser. We are going to hear in mason Cole and Chris Lewis-Evans. James Bladel and then have a discussion will hopefully you will chime in on and then for the last few minutes I'm trying to wrap up and summarize what we have heard. Let's move to the next slide please which is just an overview of the -- oh that's David's first slide already. So that should give you an outline of what we're about to do today, and with this, and without any further ado I would like to hand over to David Conrad to talk about ICANN's insight into DNS abuse. David over to you

DAVID CONRAD: Thank you, Thomas. Next slide please. So, in the run up to this plenary I was asked to put together slides that tried to reflect sort of the domain security threat landscaped from September 2019 to September 2020. If you look at the DARR reports, the DNS activity reporting reports that are available on ICANN's website the data published in those reports actually goes back 9 months, apologies for the typo. But and the request was for looking back for a year. So my team put together some general statistics, and over the past year we've seen decreases in phishing malware and botnet but an increase in SPAM, and due to the prevalence of SPAM when looking at the DNS abuse statistics it's kind of skews everything. The sort of over all take away for the year from 2019 to 2020 is that the number of abusive domains increased by about 13%, but the overall abuse ratio, because there were decreases in everything else, was more or less about the same. Next slide please. The data however that we have within DARR goes back to October 2017, and if you look farther back you can see that there are some fairly obvious trends. The trend lines there show that you know obviously the number of gTLDs is going up, and you can see various increases and decreases over time, but the trend line is pretty obvious there. In graph number 2 that's showing the number of aggregate security threats, all the things that we look at within the DARR project, which would be botnet community control. Phishing malware distribution and SPAM. You see that the trend over time is going down pretty obviously. If you look at graph 3, and you basically are normalizing based on the number of domains within a particular zone, again you see sort of a downward trend over time with a little pick up there at the end. And then graph 4 shows that the red being SPAM it still dominates everything, and the other point to note within these 4 graphs, that line either red or blue, is when GDPR was put in force. You will notice in these graphs there wasn't really any significant impact in the amount of domain name abuse, at least as detectable from within the context of DARR. Next slide please. If we then look at the individual threats for the same period from October 2017 to October 2020, again you see with the trend lines some sort of interesting artifacts. And this is in comparison to the statistics that I gave on the first page, where phishing malware and command and control were all going down. If you look back to 20 -- 20 October 2017 you get actually the opposite, that phishing malware and command and control are all ticking up but somewhat slowly. Whereas SPAM over that same time-frame is actually decreasing significantly. One thing that you want to be careful about in these graphs is just make sure you're comparing the Y axis correctly. All of all of these SPAM is about an order of magnitude higher than everything else, so that's something to watch out for. Next slide. Another data set that we collect within the office of the CTO is the identifier technologies health indicators. That was started in January of 2018 and monitors a large number of metrics that are associated with the health of the identifier ecosystem. Within that set of metrics there's one specific set, metric M2, which is focused on domain name abuse and it shows trends over time going back to January 2018 with abuses Per 10000 domains counts of abuse within gTLDs and registrars, and the ones that account for 50 to 90% of the security threats. If you look at the tables in -- on the ITHI website, which has a user interface that will perhaps remind you of the early 90's, the abuse rates there show that for example for phishing, 10% -- 10 of the registries account for 90% of the phishing security threats that are detectible. And that rates there are 0.3% Per the registries and 0.1% of the... the data there for the registrars should be taken with a grain of salt. The registrar information that we have is from our vendor, iThreat and it is collected into a database over time because we do not have access within the DARR system to the registrar information associated with individual domains. The information may be out of date, so the registrar information is something that you should use as an index, not necessarily purely accurate values. Also I should point out that the registrar, the data here -- the ITHI metrics is derived out of the same raw data that is used by DARR, plus some information associated with the registrars. Next slide please. Another project that we undertook within OCTO relevant to DNS abuse was something called the domain name security threat identification collection and reporting DNSTICR this. Started around January of 2020 aimed at collecting information associated with names that -- that registered for a pandemic related domain. There was early on in the pandemic a number of reports that a -- that there were a flood of registrations associated with the pandemic, and the implication that those registrations were being used for malicious purposes. Within DNSTICR we looked only at phishing and malware distribution as the security threats. From the period of 2020 -- May 2020 to September 2020 we were consistently collecting data, and doing an analysis of that. We discovered that through our system, that of the 134,000 registrations that were detected, about 1.7% were -- had sufficient confidence that we would call them indications of abusive behavior. And in June we actually started reporting those high confidence domains to registrars. Next slide please. So looking at what we found from June to the reporting period of June 2020 to September 2020, there are 80,000 pandemic related domains that were registered. 170 of those resulted in reports being sent to registrars related -- that were indicative of security threat behavior from our perspective, and to explain a little bit about -- more about that it meant that the domain name had been registered in the domain name system. It had at least one report that was found in one of the... provider lists and when we looked at the actual registration, the domain -- sorry website associated with the domain that it had material there that was indicative of a -- some sort of security threat, what. We wanted to do was minimize the number of false positives so of those 170 reported, as of October 6th, 87 do not exist anymore on the domain name system. They were removed. 56 no longer meet the report criteria. Either the domain is no longer resolving, or it no longer has a security threat register as available on the web sites. 20 of those don't resolve the name, NS records to the names servers don't respond to DNS queries. 7 of the 170 still appear to be malicious. With that, I am happy to answer any questions, if you'd like to take them now Thomas. If not back to you to introduce the next speaker.

THOMAS RICKERT: Thanks very much, David. We -- [inaudible] we actually have a couple of questions. I'm not sure whether we can handle them all at this moment, but let's give it a try. Elizabeth SZUDI is asking for SPAM. Does this represent... unsolicited e-mails or do the SPAM e-mails also contain and deliver other forms of tech [inaudible] and or phishing, need if a SPAM e-mail also contains or delivers other forms of abuse somehow the abuse categorized.

DAVID CONRAD: So the information that we have is derived out of reputation provider lists. They do not distinguish between the mechanism that SPAM is using to deliberate security threats. So you're seeing information related to SPAM that is reported to the various reputation providers. In our DARR reports and in the methodology document, we actually list the reputation providers we use and the specific feeds within those reputation providers to give you an idea of the information that we're collecting.

THOMAS RICKERT: Thanks, 2 more questions from. The... my members are describing, increase abuse of domains that play out from misuse of the brand names. I feel like the increase should show in phishing as well. Much of phishing is perpetuated via snap. How do the numbers reconcile this. Should they be parallel and the follow-up question for the ten registries that are the worst actors what compliance measures will be taken. Their status to date, thanks.

DAVID CONRAD: With regards to correlation between the phishing and SPAM, the information that we collect is derived specifically out of the representation providers. If someone lists something in SPAM, and it's phishing it's been distributed through phishing it's possible it will show up in the 2 different categories because it's reported in multiple places. We try to remove redundant entries of that nature but it's possible that you know, there could be some cases in which those names are duplicated. That is as far as I know unlikely. The information that we collect, we do not modify in any way right. This is information that we aggregate through a number of different providers, if folks are seeing different statistics relating to DNS abuse and security threats we would be very interested in understanding what data sources they are using to derive that information. And we can work with the DARR system to see if we can incorporate those data sets into the DARR system, and other systems that we're using. With regards to the second question, let's see -- the absolute number of registries or registrars responsible for 90% of the abuse need to be understood in the context of non-normalized data. It is perhaps unsurprising that there is a strong correlation between the total number of registrations, and the amount of abuse within those registrations. If you look at the non-normalized data, then the registries and registrars that have the most registrations will undoubtedly have the largest number of abusive domains. It's better to actually view those in the context of the normalized numbers, which are the relative to the number of registrations, when you start looking at those numbers, it -- the -- it becomes less obvious who the bad actors actually are.

THOMAS RICKERT: Thanks very much. I am afraid we need to more to the next speaker. David I suggest that while we hear from Jeff maybe you can go to the Q and A pod and try to respond some of the questions in writing? Same goes for the subsequent speakers and then for those questions that could be resolved we are trying to get back to those at the end of the session. The general Q and A. I hope that is acceptable way forward. So Jeff Bedser. And working with iThreat. Jeff over to you. 10 minutes.

JEFF BEDSER: Good morning good evening and good day. This is the effort after work party put together by SSAC about a year ago. It had a very comprehensive chart they're included quite a few other issues on DNS abuse we haven't covered yet. This is the first work product we are putting out that covers the DNS abuse issues. This is a naper has not been published yet this SSAC paper hopefully will be coming out in the next few weeks. We hoped for an ICANN69 release but internal process is not completed so we will hopefully get it out soon. Next slide please. So first of all I wanted to make sure it's clear one of the things that SSAC did in this particular work product is we invited guests from ought auditor of SSAC to participate in the work party. These were guests from the PSWG from the registry stakeholders group, and some of these guests brought in skills and knowledge that helped us understand better some of the policy issues, and some of at abuse handling issues. Apologies the app for translation just kicked on. So the group is made up of people outside of SSAC as well as SSAC itself. That gave us a rounding of people from a policy background. From DNS abuse handling backgrounds, as well as people from places like registries registrars and content delivery networks giving a well rounding of when we came up with. One of the things that you heard David Conrad speak about is the measurement of abuse data and one of the points about that measurement is not just that it existing or did exist in a particular day but one of the issues with a DNS abuse is how long it lives. For every hour for every day abuse I have domain continues to exist there is the potential for more victims. More victims means more losses etcetera and later in the presentation you will see data from Christopher Lewis-Evans about losses associated with DNS abuse. But the Internet itself is being abused to a concerning extent. There are reports across the Board you can get from media or internal or from law enforcement but there's no doubt the DNS abuse exists. No one should expect DNS abuse to stop because it's ... cybercrime will continue. Crime will continue as long as there are people to victimize. The problem we are addressing is there's erosion of trust where end users of the Internet whether they be commercial or personal or you know noncommercial, whatever activities they may be, need to trust the system and they need to trust the system and service providers so that infrastructure. The report the soon to be published will outline a strategy for reducing DNS abuse. The effort is to establish best practices and can be attained only with the co-operation and understanding of the majority of entities. DMOOEP mind that those that are contracted parties and ICANN are only a small part of the totality of the DNS system that is being utilized to do victimization. They are hosting providers. There's e-mail providers. There's content delivery systems. There's all types of places they are being used in the structure and contract the parties is an only a small part of the total ecosystem. Next slide please. So the key point of the paper are as follows. Encourage standard definitions of abuse. The paper did not make an attempt to re-define or to apply new definitions but actually went from existing definitions that were in the vernacular good enough. They described the issue. When you're dealing with a problem having a standard set of definitions of course is the best way to move forward. The next point was determining the appropriate point -- primary point of responsibility for abuse resolution. Where each type of abuse has a particular flavor to it, and where that can be resolved maybe at the registry level. May be at the hosting level. Could be anywhere in the ecosystem, but certain types of abuse will always have a certain place where they is the most appropriate point, for the abuse to be resolved. Identifying best practices it are deployment of evidentiary standards much this is tricky. Arctic that legal standards across jurisdictions have different evidentiary requirements to prove something is a problematic. Is a fraud, is a crime. But if there's evidentiary standard that says this particular incident is a command and control Botnet this is what you need to present to demonstrate it's Botnet to any one you're acting -- asking to act upon that particular Botnet domain. Establishing standardized escalation paths for abuse resolution is one where we all understand that a domain has lifecycle... different actors along the way to have it resolve. The reality also is that some places you will get a nonresponsive entity who is the primary point to get a domain resolved. So establishing escalation paths allows for different entities to come into the ecosystem and say go to a hosting provider that is -- they cannot contact. They have no availability of contact information or is nonresponsive to the contact. Where is the escalation path appropriate to the next party to try and get at that domain resolved. Again to reduce victimization the longer the more time the domain is up the more victims. Determine reasonable time frames for action and abuse reporting. Right now an escalation paths most parties allow the other party they reported to 24 hours to respond. So if a party reporting abuse I have domain enters at the wrong part of the ecosystem tan gets referred 3 times that could be 72 hours or plus to get a domain resolved. So the determining a reasonable time-frame for action will also reduce the period of time the domain is live. We also are looking at recommendation of the developments of notifier programs that will expedite and make efficient handling certain parts of the abuse system. There are many commercial entities and not-for-profit entities that do detect abuse and report it now. But another interesting trend we noted from the work party is the number of companies that are reporting abuse is going up as more and more consumers and brands are detecting abuse and hiring companies to detect abuse and there is a large volume of new players who are reporting abuse to understand the terms of service and understand how the DNS service works.

A notifier program would help with that. ... within the GDPR and it is not. This is about the entities that are actually at the different points in the control of a domain. Sometimes the abuse contact information is easy to find and other times it's not. Mechanism that would allow for availability of ease of availability for notifiers to find who to report a domain to with the evidence would be a nice addition to the ecosystem and finally creating a mechanism to ensure reasonable wall contact information. Keep that information fresh and renewed. Keep it available. So again I hope of it this report out as the work party chair to the full community in the coming weeks, and look forward to feedback from it. At that time, and Thomas back over to you.

THOMAS RICKERT: Thanks very much Jeff, and not in talk about the substance of your talks you did an excellent job sticking to the ten minutes time that we're allocated to you. That's great. I see that the discussion in the Q and A pod is primarily follow-up questions directed at David, so if you have questions for Jeff, please do type them into the Q and A pod and I would suggest Jeff that we proceed as we did with Dave, if questions are coming up that are directed at you please try to answer them in writing in the Q and A pod, will allow us to move onto the next speaker. And that is mason Cole. Mason is with the CSG is going to speak for the commercial stakeholder group and with Perkins coin and talk about the CSG perspective and DNS abuse. Over to you mason.

MASON COLE: Thank you Thomas. Can you hear me well? Thank you. All right good morning good afternoon and good evening everyone I will get started. I don't think I need the full ten minutes but let's see how the discussion goes. Next slide please. So we are here again to talk about DNS abuse. A problem that as Jeff and others have opined on that it's problem that doesn't really steam go away and probably never will. We see it occurring year after year periodically. It's magnified by outside events as we saw in March and April earlier this spring with the outbreak of COVID. You see it sometimes in the occurrence of national disasters. Civil unrest. Other world-wide problems. The common theme in all this of course is that the DNS is leveraged for illicit purposes. This is ICANN's 4th -- I believe 4th consecutive plenary on DNS abuse. It would be I think preferable for many of us if we could continue to talk about this productively but also talk about what productive solutions we can bring to the fore in order to actually do something about DNS abuse and reduce its occurrence. Next slide please. All right so in the area of statistics it seems that everybody has all you have to do is really look and line about DNS abuse and you find all kind of statistics. The most recent set that have been published forest fire SSAC sorority the Interisle consulting group report a few days ago. So during that study period which was May 1 to July 31 of this year and the study is focused on phishing but reports impacted over 99,000 unique domain names and 439 TLDs and 414 registrars. And of that total interisland identified over 60000 maliciously registered names so the phishing problem we know exists of the it may be bigger than reported although the exact size is unknown and redaction of WHOIS date is contributes to under detection of the problem. Next slide. So according to the SSAC what we know is that DNS abuse in the result and the cybercrime continues to victimize millions annually and reduce its trust in the Internet. I wanted to underline what Jeff talked about earlier. That this goes to the trust in the bedrock of the Internet whether or not the DNS can be a trusted place to go and retrieve information and do business and carry on with our work. So as a place to conduct person and noncommercial business it's important we have that truss. Next slide please. Thank you. So statistics and where we should agree. I think we can all bring different perspectives to discussion as we have for the past but you know apparently 4 sessions. DNS abuse may be going up depending on your source of data or going down depending on your source of data. What we can and should agree on though is that abuse, when it does occur has the impact we discussed on the Internet trust and it needs a proactive data driven remediation. And I put the emphasis on proactive. There is an opportunity to be more proactive and more determined in our ability to go after DNS abuse. And I want to avoid setting up an argument within ICANN about whether or not -- not whether or not we should attack DNS abuse but how we talk about DNS abuse. It's not a war we should start with each other. Our directive should be towards doing something about the bad actors. Next slide please. So progress has been made as others have said, I want to particularly applaud again the voluntary framework that registries and registrars have put into place since earlier this year I believe it was or perhaps it was last year. It's had a measurable impact on DNS abuse and should be applauded. So I want to take a moment on recognize contracted parties for good work they have done in this scenario. Next slide. So there are places where progress has not been made and we have room to improve. Voluntary frameworks are great. But they're not fully inclusive. And we know that there are always this referred to sort of 8 to 10 bad actors that ICANN says it knows about where the bad actors tend to hide. And you know it would be a useful effort to pursue the low-hanging fruit and the known bad actors to do something about abuse outside the framework that contracted parties have established. Next slide please. So let's go back to Montreal. This time last year when we had our first plenary on DNS abuse. And I just wanted to bring up an intervention by... Tucows which I thought was useful. We need to deal with the issues in front of us and if compliance is -- he's referring to ICANN compliance. Is able to effectively identify that there are specific elements of the contract that will help them to force clear bad acts that we all know are in exist tent let's talk about those. Compliance dealing with known bad actions we all agree should be dealt with. I wanted to bring that up because that's again is a proactive solution we can bring to the table here that could use some tools we already have in place to identify bad actors and pursue them. Next slide please. Okay this is my final slide. So certainly one doesn't climb a mountain like mount Everett in one step. Do you it step did I step and in stages. Similarly we have an opportunity to take on DNS abuse in stages. So in addition to the coming SSAC recommendations here are some ideas what we can do it -- something about abuse. Clean up the low-hanging fruit again the 8 to 10 bad actors that create the biggest problems in the space and we can do that now with the tools we have. We can argue concurrently or later over the definition of abuse whether or not tools are needed. We can consider incentives for those running clean registries and registrars and perhaps financial innocent I have the ICANN org has an opportunity to be... compliance function. I would like to cull and contracted parties to be proactive. ... that not only is mitigation appropriate after the fact of abuse occurring but prevention before occur sense an option. And then personally I would like to see this once so you know this cadence we've built so far this once per meeting plenary discussion perhaps we can turn that in once per meeting what we've done did DNS abuse. Those are some ideas how we can immediately move forward in the next year to have impact on the DNS abuse. Thomas back to you.

THOMAS RICKERT: Thank you very much Mason. Thanks a lot. We have 2 questions which are directed at you. And I suggest we take both of them before moving on and if I could ask you for concise answer that would be great. ... who funded the.

JEFF BEDSER: I don't I'm sorry.

THOMAS RICKERT: And LUC asks Mason could you explain how the reaction of the WHOIS is in the detection of phishing I believe the tracking of the person of interests behind the phishing attempts may be harder but the number of abuse domain names remain the same. Thank you.

JEFF BEDSER: Thanks for the question. LUC allow me to answer that if writing. That's a -- there's a lot packed in there and I would like to take a moment to respond properly to that. Thomas is it okay if I do that.

THOMAS RICKERT: Sure. And a couple more questions that remain unanswered. We will hopefully get to all of those if we can respond in writing in the Q and A pod. I know the questions have been publicized for everybody to see in the meantime. So if you ask a question please do it quick check of whether your question or a comparable question has previously been asked so that we can avoid duplicate efforts by the respondent. Next is Christopher Lewis-Evans and he will represent the abuse of the Public Safety Working Group and Chris is with the national crime agency in the U.K. Over to you.

CHRIS LEWIS-EVANS: Thank you Thomas and hello to everyone. And thank four joining us on this DNS abuse plenary. So first, if we go to the next slide.

Is why are we talking about DNS abuse? It's been mentioned it's Mason and Jeff both talked about a number of different sessions and really I think these main reason is the impact that the abuse actually has on the users of the Internet. So I've brought up some 5 stats that cover different types. Different scales of abuse. The FBI is Internet complaint center produces good statistics. They show for the last year the number of complaints that they've had so averaging you know 1,300 every day. And you know a rather large number there in losses. And that's across all user of the Internet. That's businesses. Individuals, everyone that is involved. And from the -- Within our national statistics we recorded 85% of all reported fraud is cyber enabled so you can see how much impact sort of DNS abuse can have on the harm, on individuals users of the Internet. With regards to scale of the harm that's been caused ransomware is probably the biggest form of malware out of the moment or the biggest impact and that's had a year on year increase of 715% since last year. So really really big increase in the amount of harm being caused. It's not just financial losses to individuals businesses. There's also peoples data that gets breached as a part of the... by actors. Within the U.K. over 60% of the cyber incidents recorded with data breaches were due to phishing or malware, which are obviously both key points into the DNS abuse explanation there. And that's you know recognized within the DNS abuse framework that Mason mentioned earlier. So with regard to -- next slide please. So I think I saw a mention in the chatty think by Maxime, we have a number of places where we can tackle DNS abuse, and within ICANN we obviously concentrate and the registrars on the registration and within ICANN itself and the contracts and everything else but to tackle and reduce the harm's being caused we need a whole system response. That is... Internet services e-mail providers. The ISPs. Content delivery networks of the list goes on and on. It's really really big environment that we are working in, and we really need something that helps those trying to tack this will abuse to get to the right place. I mentioned here a common -- next slide. ICANN is our common facilitator here, and we are talking about the DNS abuse. We are making some impact and it's right that Mason highlighted some of the proactive work that's gone and. And it's really key to be able to do proactive measures because it raises the bar from to get past and really make that harm a lot harder to achieve. So we have ICANN which is a common facilitator for us in the environment to this stakeholder group. But we really don't have one that covers the whole ecosystem on content side and everything else. Next slide please. So what can we do? As a law enforcement obviously I'm well versed within ICANN. I have many many good meetings with the registrar group. The registry group and other stakeholders and you can use some of that knowledge to direct you know abuse complaints appropriately. But that's not the same across the whole of law enforcement, or even across cybersecurity. You know we have anecdotal evidence of people trying to go to ICANN to effect a suspension of domains. Not the right place to go. Really unclear that you know depending on the type of DNS abuse to go to effect the change. ... content the malware might be on this. Taking the domain name down is not necessarily the first respond. However, might be the right one if it means the reduction of harm being caused to the user of the Internet. And what happens if we don't get any action? How do we escalate? And that really comes down to the common facilitator. How did we go from asking a web poster to take down content. Nothing happens. How do we escalate. Registrar doesn't respond and what is the time around that. Having these mechanisms in place is another step we can take to raise the barrier and it's really I think really important to really make life as difficult as possible for the criminal actors to effect this harm. You're not going to cure everything by being proactive. Unfortunately, there's always ways around the system. We have to have a good system so we can be reactive and we can be react in the appropriate time scale it's key any process we have is timely and can be carried out in a succinct measure. I mentioned data sharing agreements. It's key that you know we don't just turn up at someone's door and say can you give us IT data? Everything has to be appropriate checks and measures in place and data sharing agreement allows that to happen. Properly. And really, you know what you don't want to be doing is dealing with an incident and talking to a registry or registrar or Web poster for the first time. You know what you could really do is a framework to -- and set that up and have an agreement so you know the process, you know what checks and balances are needed as Jeff mentioned in his discussion earlier, have you know what standards are needed to meet what evidence is needed to provide, really really helps with the reduction in the harms scores and it's really key on that front. So for me, I think there's a lot we can still do that's based on really good proactive measures. But what we are talking about is reducing the harm that's caused by the effects of DNS abuse. Reducing the number of domains doesn't necessarily always... criminals utilize domains in different ways. It's just being aware of that to stop the harm that's being caused and with that. I would like it answer any questions.

THOMAS RICKERT: Thanks so much Chris. I will read one question from Maxime for you. Do you have any plans to... into the process? All Internet abuse happens over IP.

CHRIS LEWIS-EVANS: It does indeed and... are straight below registry in the diagram. Sorry it's a bit small. It was on the previous slide. So yes they are definitely a key part of the ecosystem. And something that first thing I engage with them very well. I have a really good relations with -- within their region, so that's something that's key. Thanks.

THOMAS RICKERT: Another question from maximum in there are a lot of calls for proactive approach. Can any one explain how to predict future and situations when nothing bad have been done yet for the domain in question.

CHRIS LEWIS-EVANS: It's very difficult obviously to predict crime is going to happen, and something that you can't really do. But if we have systems in place ready to deal with abuse once it happens that's a proactive measure so having the right systems in the place, and be able to take timely action I would say is a good step, there's lots of data activities that the contracted parties are doing, and you know within the DNS abuse framework and details some of those and probably -- well outside my remit to discuss. So I think there are a lot of things that we can do proactively to stop abuse but like you said we can't predict. Thank you.

THOMAS RICKERT: Thanks very much and I think that's probably an area we should pick up on when we discuss with the group of panelists later on.

Before we move to the last speaker I have one question if I may. You mentioned on one of your slides that 85% of fraud cases are cyber enabled. Is all that have what we call DNS abuse?

CHRIS LEWIS-EVANS: So no, it's not all DNS abuse. So that would include straightforward SPAM, which depending on your definition of DNS abuse I think comes with -- think I think some of Jeff's discussion is you know what is DNS abuse? So yeah, that's other mechanisms, which is why I also included the ICO stats which are down solely to understood DNS abuse categories.

THOMAS RICKERT: Thanks Chris. Wanted to move on but I just see the question coming in from Monica and I'm going to take the question at least because that have been complaints about gender diversity so let's try to take that on Board before we move on. The question for Christopher Lewis-Evans can you shed details on 60 per cent of recorded data breaches a tribute today phishing and malware. Do you have any details with the figures the source are for the figures and can you elaborate what means they are attribute? Perhaps you can explain the modus operandi.

CHRIS LEWIS-EVANS: So that's data published are the ICO which is the data protection authority within the U.K. And is probably about, if I share the details of that in the chat for time's sake.

THOMAS RICKERT: Thanks Chris and let's move onto the last speaker last but not least it's James Bladel from GoDaddy I and he will speak on behalf of the contract party. James over to you.

JAMES BLADEL: Thank you can you hear me okay?

THOMAS RICKERT: Yes.

JAMES BLADEL: Perfect well tomorrow to the middle of the night and thanks for including me in the discussion. One of the benefits of are being last in the program is I get to bar owe some of the points and comments made by the previous speakers and it's if nothing else demonstrates I was paying attention and taking notes throughout the session. I did want to present the contracted parties perspective which I think that as we go through the slides you will see aligns with a lot of what we've heard so far. Next slide please. So generally abuse on-line I think going to Thomas as opening remarks is a challenge for our industry. And this is a priority for contracted parties. It's indicative by all of the investments in people and system that is have been made thus far, and I think that the performance both in the numbers presented by David and of the Interisle report of the major contracted parties at ICANN democrats that investment is paying off, and that abuse generally and particularly DNS abuse is being detected and mitigated at scale. But I think we do need to recognize the distinction between general abuse, content abuse, and other types -- and other types of abuse versus abuse that is DNS specific and this goes back to Thomas as remarks about ICANN as limited role in the constraints that it has under its bylaws to focus on abuse of the DNS itself.

Next slide. So building off of that, the mission of ICANN is again to ensure security and stability of the DNS. But a lot of the abuse we discussed particularly SPAM but some of the other fraudulent deceptive practices on-line are heavily dependant upon content and that's where we start to stray outside of ICANN as remit. And similarly the ability of a registry or registrar to mitigate abuse or abusive content is restricted. And we often refer to this as the nuclear option. We only have one lever to pull as a registry or registrar and that's to take the domain name down or suspended it. And that's not appropriate for condition tent abuse. One can imagine it the scam was, orchestrated on a Facebook page we would not take down Facebook.com. If counter fit products were being sold and eBay suspending eBay is in the an appropriate response. That's when we say when we have only one lever, the nuclear option. Fortunately a lot of registries and registrars are situated in other parts of the stack. The ecosystem so for example GoDaddy is a registry and a registrar and a web host. So we have more avenues that we can use when we detect abuse. So that I think is one of the reasons why you hear contracted parties say that only a portion of the on-line abuse problem actually falls under the umbrella of ICANN's remit. But we have, as an industry organized ourselves around a number of other efforts outside of ICANN, to address various types of abuse. Next slide please.

So in September of last year this was right before the time that we were all last together was in Montreal -- a registries and registrars about a dozen of us Lauren launched a framework and DNS abuse in an effort to do precisely what some of the previous speakers said to set standardized definition force abuse. Some standard expectations for action. And identifying I think it was Jeff referencing the SSAC report identifying who the responsible parties were for various types of situations and what a typical mitigation response would be.

We have since grown to over 50 signatories to the framework and I think that as Mason noted it is having an impact. It is pushing the abusive -- I want to say abuse tolerant or perhaps those registries and registrars who were less capable, it has helped to kind of build up the overall capability of the industry, and pushed these abusive actors towards the margins. Just yesterday, all of the original participants and some of the new signatories released a year one update. You can find it at the... abuse framework.org and it explains what our experience has been operating under the framework and some of the abuse trends. So rather than bombard this session with charts and stats I encourage folks it visit that link and get an update from each of the members of this framework. Also, in 2019 a little earlier I think April or May the Internet jurisdiction policy network publish add white paper similarly outlining all the challenges of detecting and mitigating DNS abuse, and those definitions align closely to what you see in the DNS abuse framework however they included... hosting which is not included in the framework so there's one point of diversion there. Outside of DNS abuse when we look at content there are numerous industries Alliances and associations and coalitions and you know task forces. This is an all kinds of other things that may maybe folks are familiar with and maybe not. But are targeting specific categories of abuse like SPAM, like child abuse. Counterterrorism. Recruiting financing. Pharmaceuticals. The point of the bullet is just because you don't see the actions occurring and a category of abuse under the umbrella of ICANN doesn't mean thank you work is not occurring at all. And, in fact, a lot of contracted parties will switch hats and participate in the other organizations and perhaps as a web... for other situated company. Next slide please so just current state of affairs. Look this year has been a rollercoaster. And the entire world raced to pivot on-line mostly as a means of is your survival in response to the pandemic and we are speaking specifically of small businesses. Everyone is familiar with their favorite restaurant pivoting to take out or curb side model to stay in business. For those of you with children this today's motion schools you know 2011 completely transform that experience political and civic and religious organizations are all moving towards more virtual virtual footprint rather than physical and the same is true for ICANN. And I say that because our industry, contributed to that great pivot. These are trends that were already under way but COVID-19 accelerated what was happening over decades and compress it had into months, and off of course the hope is when this is over we will all be a little more flexible and capable in bouncing back from that transformation.

But we should not be surprised that all of the criminals and fraudsters and bad actors and opportunists followed that transition. They transform as well and they evolved their approach and their tactic toss follow their the victims were and if the victims were no longer participating in a physical or mostly physical economy, that they would re-emphasize their -- the virtual aspects and the cyber aspects of the attacks but all of that said, the data does not indicate that the sky is falling that the Internet is falling apart. Far from it. Next slide that goes back to some of David's statistics but you know our industry saw a couple of upticks in phishing reports and I think one of David's charts was a trend line. There were a couple of outliers dropping the average up and that corresponds with some peeks we saw in the spring and then a couple of in the Summer as well. Over all I think that we've seen a modest growth and I'm now probably being more specific to GoDaddy than the industry as a whole because I don't have centralized statistics but we are seeing something in the order of 15% growth. Nothing that looks like an order of magnitude jump in activity and nothing that would indicate that some new or novel type of attack had been developed. Right now GoDaddy is processing about 2000 phishing reports per day. That's not domain names. That's not specific incidents. That's just reports, and some of those are I should note are coming from for example Internet tool bars that send a lot of duplicates. So going through each of those individually and eliminating duplicates is a significant effort, as well as the noting that even when we account for to only about 8 and sometimes less than 3% of those reports are actionable.

Either they're no longer functioning or they're missing key bits of information. So there's a lot of noise in the channel. It's very difficult to get to the specific and legitimate incidents and maybe that's something that we could look at operationally, and co-ordinate perhaps with OCTO and across industry to get better at zeroing in on focussing on the legitimate problems. Next slide please. Just a little bit of a word. It's not exactly related but it is I think part of the same theme is focussing on the scams and fraud campaigns associated with the pandemic. The these of course dominated the headlines in early part of the year, and I think Mason alluded to the peaks we saw in March and in April when almost everyone was in some sort of a lockdown. I think that the bottom line here is that these were content focussed. And we're not particularly new. They had a new wrapper you know where they were trying to take advantage of the views of the day, or prey upon the fears and anxieties that folks are in the early stages of the pandemic. But underneath it was the same old phishing and fraud attacks that we have been dealing with for years or even longer. And so in our case for example in GoDaddy we did not feel that we had to scramble to develop a new terms of service or a new policies or new capabilities. We found that our exist toolkit worked well against the COVID-19 scams this year and a lot of that mitigation again was happening as a web host and not necessarily be via attacks on the DNS. I should point out -- and there was question back and forth to comment from Chris and from Mason about preventive an are proactive steps to be taken -- we received a lot of proposals and even pressure from political figures early onto you know, just block COVID from the DNS. Don't let anybody register a name that has to string. Don't let any one register coronavirus and they're only going to do bad things with it, and it's a very -- I recognize the allure of that type of a solution. But I think I need to point out that it's much more complicated than that in the field. Most of the harmful and abusive domain names we've seen don't explicitly reference COVID or coronavirus so they wouldn't be detected by a method like that. Conversely we sought a lot of public health authorities and local news outlets and local governments using domain names with those strings for official news and updates and instructions. So we need to I think -- hopefully the sophistication of the ICANN community is when we see outside of ICANN calls for blocking strings in the DNS as a solution to a particular problem, I think all of us recognize that while that's tempting, that is not necessarily an approach that is either effective or has an acceptable level of let's say false positives and collateral damage. So next slide please. I think this is my last. Bottom line is obviously abuse is something that's important. It's not being swept under the rug but the role within ICANN and our role as registries and registrars upped our contracts with ICANN is fairly constrained. We have more tools we can bring to bear in our arenas. We think that there's value to discussing these topics at ICANN to facilitate the discussions, you know get more perspectives from other dimensions of the community, the research that I think OCTO and SSAC are doing is vital, collecting some an aggregating some industry wide statistics is helpful. But I think -- and I don't think it is a surprise to any one to hear this. You're going to see some hesitation from contracted parties about launching new policy development efforts or contractual amendments in this area. First I think that we need to very very tightly define the problems such that it clearly fits under the remit of ICANN, and then secondly we would have to -- and I this think goes back to the quote from Elliott that was part of Mason's slides -- about making sure that we exhaust all of our existing contractual mechanisms that we could bring to bear upon the small number of bad actors where all this stuff is concentrated as oppose it had writing new policy that is may or may not be tested against these problems if we know that there are some methods that are proven to work how can we push those auto they are more broadly adopted and implemented? So that's my deck, Thomas, and thanks for including me. And thank for hearing me out.

THOMAS RICKERT: Thanks so much James. James actually we do have one question in the Q and A pod directed at you. I would like to if you from Marcus V. Question for James. Of would trusted notifier arrangements be a good mitigation for all the noise you mention.

JAMES BLADEL: I think so. I think trusted notifiers are a good way of having a filter over those sort of false positives and duplicate reports. Anything that we can do to keep our teams and our tools focussed on the actual threat and kind of unclog the pipeline is worth support. Sure.

THOMAS RICKERT: Thanks very much. Now we have around 17 minutes before the top of the hour. So I see that the questions in the Q and A pod are being answered by the panelists and I would like to let that take place in the Q and A pod. Just one point that Jeff Neumann mentioned that was a question surrounding the format of these plenary discussions and that they should I'm at producing recommendations or concrete results. So I think we've all heard the same presentations, but I am not sure whether we have the same take away messages so let me try to tease it out a couple of points hopefully that we can agree on so that we have something, if you wish tangible for us to build on. The first point that I would like to get some feedback from the audience on or from the panelists on is regarding the definition of DNS abuse because the roles and the actions may they be proactive or reactive that can be taken by the various... depend on that. So it reference was made both in the presentation from Christopher Lewis-Evans, as well as in James Bladel's presentation to the DNS abuse framework, and that actually highlighted a couple of points being malware, Botnets, phishing, farming, SPAM, with some qualifications to the SPAM topic. Wouldn't it be an idea -- and this is a question from Jeff -- that you and your report with the SSAC probably just build on that because you mentioned that you were working on definitions? So I guess it would be great benefit from hopefully to everyone if we had a common understanding of what constitutes the DNS abuse and whatnot? And for those who want to ask their own questions, please put them in the Q and A pod. I've been advised by ICANN staff it would be better given the limited amount of time that we have that we don't try to unmute individual microphones for them to speak and I will make sure that as time permits your questions will be read out and discussed. Jeff, is that something that you can respond to?

JEFF BEDSER: Sure Thomas and thank you. So a common framework for definitions is a core for solving the problem because then when there are new types of cybercrime that may not fit in the core definitions we have the ability to define it, put parameters around it and address it so I think that is a very key component to any type of solution regarding DNS abuse as a firm repository of definitions that everybody can call to when trying to determine what a particular fraud or domain event is tide to, aen what category.

THOMAS RICKERT: Has the SSAC taken a look at the definition offered by the DNS abuse framework document which basically builds on the... jurisdiction work?

JEFF BEDSER: Thanks Thomas. Yes it actually calls those 2 works out specifically in the sections on definitions.

THOMAS RICKERT: That's great. Would anyone else from the panelists like to chime in to -- not to agree, but to state an opposition to the definitions or is there -- or can we take silence if there is silence to that question as an agreement that probably the DNS abuse framework is a good starting point for the common definition of DNS abuse? So I'm not looking at any specific panelists since we only have a limited number of panelists. Please open your microphones aen speak out if you think that these definitions are not properly -- or are missing anything.

JAMES: I can jump in. I think it's good starting point. I think Jeff mentioned the SSAC report calls for some additional work defining a definition. I think that there's some questions in the chat about where do we go from here? What is the next step? How do we present the panel from being rinse and repeat for ICANN 70 and 71 and 72? And perhaps the way to get off the merry go round is to kick-off some discussion of the definitions starting with what's in the framework based upon the SSAC report, and then including in that the analysis of why it is or is not appropriate for ICANN in its kind of limited role and limited mechanisms is registries and registrars to take on that particular definition or whether -- and I think this is a SSAC report as well -- the second point is whether that belongs to a different responsible party and how to get it over to ha responsible party and maybe that's the offering we can at that I can from kind of these -- I'm just responding to the [inaudible] repetitive ground hog day type of panels.

THOMAS RICKERT: Thanks very much James. Mason please.

MASON COLE: I wanted to follow up with James. I agree with him on the whole -- the framework and the approaching SSAC report are good starting places for the definitions. I just want to repeat what I said in part of my presentation which is I don't want to see us get bogged down or overly bogged down in the definition while abuse continues to carry on. It's now is the time to actually take corrective action and not wait for proactive action while trying to define a problem. So I just want to make that clear to the community that the CSG and others interested in this problem would like to see ICANN take some action here. And not you know to Michaela as point I think we can meet and meet and moat and meet and talk about DNS abuse but what we need to do is take some concrete steps so I hope that is the case and we don't get too bogged down and the definition part.

THOMAS RICKERT: Thanks, Mason.

JAMES BLADEL: And maybe this is appropriate to have you know panelists going back and forth or maybe it isn't I don't know. But you know I think Mason I think I think there is a point of divergence for us is that that sounds a lot like ready fire AIM and having a definition and understanding it we have a clear remit. You know is necessary in order to take those next steps. I just want to emphasize because I want to make sure it was -- maybe I didn't cover it very well, or communicate it well but there is not an absence ever work. They may be miss visible in ICANN because they're occurring in other arenas with different sets of parties and companies, but we are not kind of stuck in the mud necessarily. We are just doing things in other places.

MASON COLE: I appreciate that James. I don't want to have a back and forth on the panel either but you know I do think there are no notorious 8 to 10 bad an actors we have talked about for many months. Maybe there are some other things going on in the scenes that you know contracted parties are taking care of we don't see, but you know I don't want to have a ready fire AIM approach. I want a proper approach to DNS abuse and I don't think we're quite there yet. Thomas I will yield thank you.

THOMAS RICKERT: Thanks Mason and James. I guess that with folks be waiting for the interaction wean the panelists. So I'm happy for that. I think nobody should take policy work as an excuse for not taking action and I think that you know at least from my discussions with contracted parties a lot of them are -- all of them at least those who presented here are doing quite a bit. But I think that the definition part nonetheless is crucial to get things right. We need to make sure registries and registrars have their place in the ecosystem and can take appropriate action according to what they can. Same with ICANN. For example ICO the association, I would, with also operating a... complaints from the general public with CASM primarily and James made reference to that in his interventions and before the panel I reached out to head of that and asked if they rather go to registries and registrars or go to hosts and they said they prefer go to hosting companies and ask for take downs because they want to make sure the illegal material which is sometimes in many cases evidence of on going abuse is not further distributed at the source. All right so I think we need it get that right. The in next point I want to touch on briefly is there seem to be discrepancies in the statistics. Some say the number are going down much the others say the issue is not getting smaller but it's more like or less the same. David, you've heard when the panelists had to say and you also followed the discussions in the chat and in the Q and A pod. Can you make sense of the different message that is we seem to hear what when it comes to statistics.

DAVID CONRAD: My assumption is that we are looking at different parts of the elephant, right. There's and questions of what exactly is DNS abuse. What exactly are people measuring? One of the comments that I made in the chat is in response to indications that certain groups are seeing far different numbers than what we are seeing within our data sets, we would be very interested in seeing other people's data sets. We are trying to collect as much data as we can to provide information to the community to help inform these discussions. And the more data we can provide to the community, hopefully, will lead to better understanding of the actual realities behind DNS abuse as opposed to anecdotes. So from my perspective you know, the data that we have suggests that over time the DNS abuse has been decreasing. Others view that DNS abuse is increasing. And it would be interesting to me to understand you know what data sets people are looking at that results in those different statistics.

JAMES BLADEL: Thomas you know I think some of it is just an indication of how uneven the problem is distributed throughout the DNS and throughout the Internet. I noted that on David's slides there were some outliers, and those corresponded with some spikes, I think that we saw internally in our data set. So it could be the case where sea level couldn't change but a couple of too times a year it floods. That's maybe some of distinctions it's not that the numbers are different but we are looking from a different angle over a different time period.

THOMAS RICKERT: Thanks very much James. I have up with more question for Chris. Now that we've heard from James and from David as well that it would be useful to get statistics or as much data as possible to try to make sense out of the different data stores and make a distinction between what's anecdotal and was found in facts are there knew discussions under way for the law enforcement community to maybe align with the industry in a common recorded format or definition so we have the same fact base I'm sorry our policies on or responses on.

CHRIS LEWIS-EVANS: Yeah thank you Thomas. So law enforcement is undertaken a big step change in the last few years to be more transparent about you know crimes that are reported. How they are recorded. What are the actual underlying causes of those and the FEI's IC3 reports are very good indication of these. How we align those globally is always going to be fun. I think we struggle enough within ICANN to you know agree on a set standards for data recording, so I think that's work certainly that needs to be undertaken, however, I think you know more importantly is getting the data out there and just being as transparent as possible about what is being caused and that will allow us to work more collaboratively and take effect across the whole ecosystem.

THOMAS RICKERT: Thanks very much Chris. We have 2 minutes left in the session so let me try to summarize and adjourn. So I think what we heard are a couple -- a lot of comments which I think is great. I think there's alignment within or among the panelists but also beyond that it would be great to have comment definitions of the issue that we common statistics or common data points, I think it's also become clear that any suggestion that is the issue is bigger or smaller or different should be provided together with evidence for other data sewers that is can be correlated with what we have or the request or pleas for other action on really welcome not merely anecdotal so I this I that would help a great deal. I would also like to get back to one point that Jeff mentioned in his presentation and that is education. We need users that are... for phishing or... other bad things going on. So I think it needs to be a combination of different things, of different remedial actions that can be taken by the various actors in their respective roles to the ICANN contracted parties law enforcement or others. But I think that if we can probably work on those that would be a good starting point. And I have no involvement in the creation of the DNS abuse framework paper but it looks like a lot of folks are actually pointing to that so maybe as a recommendation that contain as the basis for discussing things low are like definitions for trusted notifier systems and all that. So I think that we should not re-invent the wheel but build on previous work. Finally I would like to thank the panelists. I would like to thank the ICANN staff and in particular the technical team for ensuring that the session could be held so smoothly without any technical issues, and I would like to thank you,... it's very difficult to follow hours and hours of meetings remotely without the benefit of meeting people in person over a coffee break, so thank you for bearing with us. Thank you for your attention, and with that I would like to thank you all again, and this meeting is now adjourned.

[END OF TRANSCRIPT]