COPENHAGEN – How It Works Understanding DNS Abuse
Sunday, March 12, 2017 – 15:15 to 16:30 CET
ICANN58 | Copenhagen, Denmark

STEVE CONTE: The last session will be in this room at 5:00, I believe. Today, this session is John Crain from Office of the CTO. He's the Chief Securities Stability and Resiliency Officer. That's a mouthful. CSSRO?

JOHN CRAIN: Cicero like the philosopher. Who had his head chopped off.

STEVE CONTE: A little bit of housekeeping. John said that if you have any questions during the presentation, go ahead and raise your hand. I've got the second mic. I'll be sitting back just watching. We're preferring that we don't ask questions off the mic because we do have remote participants, so I'd like to make sure we're recording the session. I'd like to make sure that we capture all the questions, as well. So with that, John, I will hesitate for one more second and explain something else. John, with that, I'm going to pass it on to you.

JOHN CRAIN: It's all right. I lost the clicky pointy thing. That's a technical description for this device. So I'm John Crain, CSSRO is the title. It is a guy out of Roman philosophy who had his head chopped off. I wasn't joking.

So Steve made me come and give a presentation because he likes to make all come give presentations. And thought what I'd do is I'd do an introduction-level talk about DNS abuse because it's a term that gets thrown around a lot, certainly in ICANN circles. We hear people say things about DNS abuse.

And as I said, it is introductory-level. So don't expect any deep tech here. So if you came here for a highly technical discussion about how to disassemble malware or anything like that, wrong torque. Go to the bar for an hour or go find something else interesting to do. But hopefully, it will pique your interest and get you to go and do some further research or to come to talk to me or my guys about things if you have specific interests. I'm going to see how far this works because everybody sat at the back but it doesn't work in my classes because I just walk to the back and talk to you.

So we're going to go for a few different things. We're going to talk about what is DNS abuse. I'm going to try and talk a little bit about how that fits into the ICANN context, i.e. the policy realm, show you a few examples and I'm going to give you a bunch of

links of things you can go and look at if you want to learn more. I'm going to try and keep this relatively short so we can actually do questions and answers because that's much more fun than boring PowerPoint. I'm not a fan by death by PowerPoint, so I'd rather have a conversation.

So anytime you have a question or a comment, raise your hand. Steve will pick up a microphone and run as fast as he can to you so that you can ask that question. But please, once he's done that, if you have a second question, wait until he's sat down again. He wants the exercise.

So what is DNS abuse? It's a wide range of things. There isn't actually a single definition of DNS abuse. It's different things to different people. Some types of cybercrime or online criminality, people consider DNS abuse, and we'll get to some of those. Hacking, if it's against DNS systems, it's considered DNS abuse. And the term we use a lot at ICANN is malicious conduct, which is often another word for cybercrime.

There is a terminology and it's intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and the procedures used to register or resolve domain names. That comes from one of our DNS abuse documents and was clearly written by a lawyer. It's quite long.

Simple terms, to me, DNS abuse refers to anything that either actively abuses the DNS infrastructure and systems, the ecosystem, if you like, or it misuses the protocol and the registration systems and people using names for malicious purposes. And depending on who you talk to, they will use the term to refer whatever is in their interest. So you'll hear it used in lots of different contexts.

So some of the things that we often see, phishing. Phishing is really an e-mail thing but people use names and I'll get back to that. Malware command and control, data exfiltration. Did people know you could exfiltrate data using the DNS? DNS has the ability to include text files in there or text. There's a text record. You can put anything in text, so you can actually exfiltrate data in the DNS. Malware distribution, exploit attacks, various scams that use DNS names. Selling counterfeit goods, farmer, and even e-crime infrastructure where they have their own DNS infrastructure, etc.

A lot of the time, the names themselves aren't really the problem. Right? The name hasn't been registered for malicious use. A lot of the time, there's compromised domains. So when we talk to people from my group, we tend to differentiate between when we're talking about names. Names that are registered for malicious use, and we call them malicious names, are names that are being compromised and those are really

victims. It's somebody else's name that's been compromised. And all of these attacks can use both types of scenario, either a name that they register for it or they go and break into somebody else's name. I'm not going to go for all the different ones.

Some of the well-known kind of attacks when they actually attack the DNS – has everybody heard of cache poisoning? Cache poisoning is basically when they change the records on your DNS server in the memory to give it different answer than it should.

Indirection attacks, where they actually change things in like the host file or in the memory. So that when you try to connect something in the DNS on your computer, it doesn't even go to your resolver, but it actually gives a bad answer. All of these are ways of giving you different answers than you should expect.

Denial of service attacks. They both use the DNS and attack the DNS, and I'll get back to more of that. And lots of exploitation attacks within the DNS server software, making them fail or making them give bad answers.

So why does ICANN care about this? Obviously, it's got the word DNS in it, so anything with DNS we get involved in. So what happens in the DNS context?

DNS abuse or malicious use always comes up in ICANN discussions at some point. There are two or three panels and I'll get to those later here at the ICANN meeting that touch on this very topic. Anybody ever been involved in a discussion about how bad the data is in the WHOIS? A few people, right? WHOIS accuracy discussions, which also oft get looped into this because people who do these kind of DNS abuses don't normally use their real names in the WHOIS, has been going on since ICANN was first started. It was one of the first sort of abuse issues was the problem with WHOIS accuracy. That discussion goes on today and will probably go on for quite a while. It's a hard issue.

You know now we're talking about changing the whole protocol, which we should have done like 20 years ago, in my opinion. But that's an abuse issue. It's like not having accurate ability to see who has registered what is actually an issue if you're trying to deal with abuse.

Governments. Everybody knew that we have a Governmental Advisory Committee here at ICANN? One of the things that governments do, because it's kind of their job, is they worry about public safety. Public safety issues. That's why they have agencies like law enforcement and things like that. So they, of course, always worry about public safety issues, as do people in the industry and pretty much everybody.

Abuse issues are, of course, public safety issues, especially if you think about some of those things that were listed. A clear one that we hear a lot about here is things like all these people doing pharmer and drugs, we've had a lot of discussions about that, but also malware, etc., stealing people's data, ransomware locking up people's machines. These are all public safety issues.

So you can go back, you can actually go back further than this, but this is the one I decided. Back in 2013 in Beijing, in the GAC's communiqué. Is everybody aware that the GAC operates by issuing communiqués to the Board and the community? Pretty much every meeting, they will put out an advice or a communiqué to the community. This one's from Beijing, which I think was Steve's first meeting long ago. No. This is another meeting.

STEVE CONTE: No. This is the other one. Mine was 2002.

JOHN CRAIN: 2002. Wow, a year older than I thought. So am in. Wow. Time flies. But here they said that they wanted registry operators to ensure that terms of use registrant include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark, or copyright infringement. Fraudulent or

deceptive practices, counterfeiting, or otherwise engaging in activity contrary to the applicable law. And I pick this one out because it becomes relevant a few slides later.

Pretty much every Governmental Advisory Committee communiqué has something in there related to public safety or abuse, so it's a hot topic. Always has been and always will be. These slides will be available, so don't try and write down the links.

Recently, and I can't remember how recently, I come to all of these meetings and they become a blur. The government formed a working group, Public Safety Working Group, the PSWG, and they'll be meeting at this meeting. And that's public safety individuals, so it's not just law enforcement. Right? Public safety goes much broader than that. Advising the GAC and providing input into these communiqués that then come into ICANN. They come into the policy discussions.

Policy discussions eventually lead to policy and then they lead to contracts. That's kind of how ICANN works, right? You have the policy discussions and then, eventually, everything ends up in the contracts. So, if you look at today's base agreement for the new TLDs, you'll see a couple of specifications that are interesting. I've been at ICANN since, well, a long while. And in

the early registration agreements with both registries and when we formed registrars, we didn't have a lot of this stuff.

Specification 6-4. I'm not a lawyer but I can copy things from legal papers. An abuse point of contact and malicious use of orphan records were both included in the contract. These are things that registries should supply and should worry about.

Specification 11-3 is all about public interest commitments. Now, I'm not going to go into in-depth, but if you go and read that agreement, you will see very similar wording to that Beijing GAC communiqué. It says that registries will have in their terms of agreement, i.e. the people that they register names through them with, things like you shall not use this name for phishing, for malware, botnet control, and things like that.

It's not word for word but it's pretty close. So you can sort of see how the process works doing math. So three or four years ago, a communiqué came out, had some wording. We went through the new gTLD process and a lot of wording found its way into the contracts. The registrar accreditation agreement, those are the other contract party, has similar things. 3.18 has an abuse contact, and I think this is 11-3B. My colleague put this in here and I didn't think to go and look at exactly which point it was. Duty to investigate reports of abuse. It may be a different one. And take reasonable steps. Doesn't say what those are.

But, obviously, everybody's worrying about abuse. If you're a registry, a registrar, obviously in the SSR team. If you're in the GAC, if you're from the ALAC. It doesn't matter where you are in this environment. Everybody worries about abuse. It's a big issue. You might call it cybercrime. You might call it phishing. You may have a specific area, but abuse is big.

There are three sessions that I pulled out. One of them looks like it's happening tomorrow at this time, a cross-community session. That means lots of different areas coming together towards effective DNS abuse mitigation. That will be interesting. Should go and join in that, give your input, listen to what they're saying.

Tuesday, the statistical analysis of DNS abuse and study results. There was a study done about how abuse is, I guess, in the new TLDs. I don't think you're going to see a lot of results from the study but a lot of discussion about how you actually go about measuring that. Turns out it's not as easy as people often think. We also have projects for abuse measurements and they can get quite complex. And then on Tuesday, we'll actually be doing the same discussion I think here.

There's a GAC Public Safety Working Group discussion where they will talk to the GAC about what their next recommendations, etc. will be. Those are the kind of three

obvious abuse sessions here at ICANN. Now, there are more. There are more security ones. You have a question?

[SUBA SUBRAMANIM]: My name is [Suba Subramanim]. He was talking about some abuse measurement just now. Is there any study done to measure abuse in the domains registered with one registry in comparison with domains registered with another registry? You don't have to name the registries. I just want to know if a certain domain is more prone to be abused if a certain top-level TLD has more abuses as registrants. Is there any such study? And if so, what could a registry do to minimize such abuse of registrants?

JOHN CRAIN: Two answers to that. So there's two questions. The first one was: are there studies? Well, there are lots of people that measure abuse and they sought that abuse in various ways. One of them may be by the TLD or the registry. For each of these, you've got to go and look at them and decide on the quality of the data, read the methodology, etc., but they are out there. Some people agree with them, some people disagree with them, and it's often around the science behind it.

We ourselves – we'll be presenting on this I'm not sure exactly which one of these sessions – are looking at registering various

types of abuse. Before you can register abuse, you've actually got to decide what abuse is. Right? And as I said at the very beginning, nobody can really 100% agree. So those various lists that I put up of different types, there are various data feeds of people measuring that abuse, and we're looking at those.

Now, when it comes to how do you best deal with that, there is a session tomorrow on preventing abuse. Right? And abuse mitigation. So, that's an ongoing discussion. Now, today if you have an abuse issue, you can go to the registry or registrar because they both have abuse contacts and you write to them and they have their own abuse mechanisms. But we're talking a lot more now than we have in the past about how do you actually do that, and the registries work together with the registrars. I don't work at a registry or registrar, so I can talk to their specific technologies that they do.

One of the things I've seen a few registries do is they take these feeds and then they look for the worst-offending cases or the cases within their TLD. They look at the abuse reports, if you like, and then they decide whether or not to take action based on some algorithm. I don't work there so I don't know what algorithm there is.

There are registries that take action against abuse and they have their definitions of abuse normally in their acceptable use policy

and, often, it's based around these elements that say that you can't do X, you can't do Y like phishing and malware. So, it's getting better. That's definitely the case because I can see that. In some registries, when they do this, it gets better. But there isn't a standard mechanism for this.

Go to the session on mitigating abuse. It's going to be interesting. I want to be there. I want to see that one. So, these things are under heavy discussion at ICANN. Obviously, everybody has an interest in this.

I'm going to go through a few examples of abuse. Not too many because we could go all day.

The first one is malware, and here is a long diatribe. But basically, and this is from the Safeguards Against DNS Abuse document. What they're basically saying is that when people are doing nefarious activities or criminal activities online, that they use the same resources everybody else does. If you're going to perpetuate some kind of badness online, you're going to use IP addresses, DNS names, routers, hosting servers. No different than somebody who is doing this legitimately for a business.

Now where they do differ slightly is that a lot of the bad guys have no worries about infecting your machine or hacking into your machine and using your machine for abuse. Normally what they do that is, of course, malware, which comes from the term

"malicious software." So, they're using all the same services we use. So, of course, they abuse the DNS, just like they abuse hosting services and other places.

Malware is kind of the software they use to infect all these machines. Now, obviously, we don't want people infected, but it also actually affects us in other ways as an industry.

Botnet command and control. When you get to all these thousands or, sometimes, millions of machines and you combine them together and control them in one go, we call that a botnet and that comes from the term "robot network." We're actually not that clever when we make all our little short things. They're normally just cut off from words.

What's interesting is the way that sometimes they control these botnets. So, if you've got 1 million machines, you need to go and send them all commands at the same time and get them do things. And they can do anything with this machine pretty much that you as a user can.

What's some of the more recent – and I say more recent, I'm talking about from sort of the mid-2000 onwards – botnet command and controls do, the malware has this, is they use something called a domain generation algorithm or a DGA. So, if you hear the term DGA… Who here loves acronyms? You're at the wrong place if you don't love acronyms. ICANN loves

acronyms. A DGA is a domain generation algorithm. It's a piece of software in the malware that generates names. I said I wasn't going to get into technology, so I'm not. And then so based on a particular date or a time, they will make contact using the DNS with a machine that is going to control them, send them commands, the controller.

Now, those DGAs, some of them may only generate 1000 names that they'll use over the next year. Some of them, like Conficker, will generate 50,000 names a day, and those names may be in more than – well, they were in more than 100 different registries. And this is actually a sample from 1st of January, 2013, from a variant called Conficker A. So, I can publish these because this is years ago. They're not going to be using them because they were only going to use them on that particular date.

Imagine you got a string of 50,000 of these names every day. If you want to stop the bad guys from controlling that network, what do you have to do? You have to stop them being able to send data, which means you have to be able to stop them from registering and resolving the names. You have to make sure that those 50,000 names don't work that day. All of them. All right?

So, if you want to stop the bad guys, you're trying to stop 50,000 names a day or 1000, depending on the code, and they need to get one because they only need to talk to their infected machine, ones to give them commands. This happens quite

regularly that there are actions often by law enforcement, sometimes by large software companies, trying to disassemble botnets.

Has anybody here heard of Avalanche? A couple of people. Avalanche was a botnet and an action by law enforcement led by the German law enforcement through Europol to break a botnet. And part of that botnet was DGA. And if you read the press release – and there's a link here – it says that they blocked 800,000 domain names. And people read and they go, "Oh, my God. They took 800,000 domain names away from somebody." It's not what they did. They prevented them from being registered.

Now, if you go back and you look at those strings, you can see that they're mainly random characters. They're typically not names that people use. I can't remember precisely with how long the names were for Avalanche, but they were 13 or 14-character long random strings.

Why do we care about that? A couple of reasons. Firstly, they're kind of making abuse of the way the registration system uses and the way the DNS works. So, that's kind of an abuse. But to block those registries who then get involved and they get court orders and things, now have to go and block thousands of names. So, they're affecting the system. They're abusing the

DNS system in at least two ways. And this does happen on a not a daily basis, but a fairly regular basis.

Like I said, Avalanche is the latest one, I think, that has press releases and things around, but there've been many since. And that happened November the 31st, Avalanche, last year, so it's fairly recent. If you're interested, the link is there.

Another reason we care is something called DDoS. That was in the list. Has everybody heard of DDoS? Distributed Denial of Service attack. Not fun when you're operating infrastructure and somebody launches one of these against you. So, a DDoS attack or a Distributed Denial of Service attack, is basically when you use these thousands of machines to attack a single, or sometimes multiple, dedicated target.

So, if I've got a botnet and I've got a million laptops or home computers or home cameras or whatever they are, devices, and I send one megabyte of traffic from each of those toward somebody, that's a lot of traffic. DDoSes today reach proportions that I guarantee you that none of your networks will withstand. I mean, we're not talking about single gigs here. The largest ones are in the hundreds of gigabytes. And if you don't have good contacts with your upstreams and people who are smart about filtering traffic, etc., your average network is not

going to do too well. We've seen recently that were pretty bad. They get pretty big and I'll show you some more on those later.

Because of how the DNS works and the characteristics of the DNS, it's actually a really cool medium for launching these attacks. So, DNS uses something called UDP or the User Datagram Protocol. It's basically a fire-and-forget protocol. You send the packet and you're not actually expecting an answer. It's also quite possible to send a very small question and get a larger answer.

I got pretty pictures here and, hopefully, it works. I didn't build this slide set so or this one, so if it doesn't work, it's somebody else's fault. So, you got an attacker, you got a bunch of botted machines or zombies, you've got some resolvers, you got name server at bar.tld, and you've got target name server, your victim, and we're using 10.10.1.1. Hopefully, everybody knows why that wouldn't work in the real world. That's a private IP address. And we're using some open recursive resolvers.

That's a resolver that is meant for answering questions on somebody's network where they've not bothered to lock it down, so anybody can answer that server's questions. So, I'm the attacker, I'm either doing peer-to-peer or I've used my DGA to get my domain name, and I connect to the infected machines

and I say, “Go ask some questions.” So I say, “All of you infected machines, go ask a query for foo in a domain bar.tld.”

And I ask these to some open recursive solvers and I say, “My IP address is 10.10.1.1.” Because surprisingly, you can completely lie about what your IP address is. What I’m doing here is I’m saying, “Excuse me. All you folks over this side, could you all send like throw tomatoes at me? And I’m actually this gentleman over here. So, if you please just throw all your tomatoes at me, it would be great.”

That’s basically what you’re doing. And lo and behold because the Internet’s a beautiful thing, they all ask name server.bar.id. Say, “Hey, what’s the record for foo.bar.tld and I’m 10.10.1.” They respond to the open recursive resolvers and they’re going to send a 4000-byte DNS tech RR because they already built that in there because they own that server.

And all of those answers get sent back, or not, to 10.10.1.1. They get sent to this guy who says, “Who is the poor target?” And if you’ve got a million machines doing this or even a few thousand machines, it soon becomes overwhelming. We call this an amplification attack because I’m sending small queries and getting really large answers. And we see this in the wild. This exists.

Most DDoS that I've seen lately are much more complex than this, but this is how they use the DDoS. They do other things, as well. And UDP is the User Datagram Protocol is not just a DNS thing. There are other protocols like network time protocol that also use UDP and attacks are done in a similar way against those kinds of services.

That's somebody abusing the DNS. Now, imagine if that 10.10.1.1 was your name server or your TLD's name server or the root servers. These are attacks using the DNS against the DNS. I think there's very few people that would have a problem with saying that this is a form of DNS abuse. It's not what most people would normally mean because most of the time, they're talking more about the things like phishing, etc., but this is a form of DNS abuse. And having been at the end of it, I don't like it. It's not fun when you get DDoSed.

So, pretty pictures. I've been told if I'm going to do death by PowerPoint, I have to have pretty pictures. So, here's some company, digital track. They do every day, they draw a diagram of all the DDoS, and you can't really see much on there. Even if it was nice, bright colors, it would just be a big mess of lines. It's a lot of DDoS happening. A lot of this may be against small companies or it may be against infrastructure. It's pretty prevalent. It's not good because I think that's where these guys are… That is interesting, isn't it? What did Nebraska do? I think

it's country-to-country. It's not network-to-network. They just happen to put it in the middle of the country. So, what Nebraska did was they got stuck in the middle of the country.

You'll see at the bottom there's sort of a time chart. I wonder if I have one of these, ooh, pointy light thing. There's a time chart here and it just shows you the attacks over the day. It is the Chicago skyline. It's actually this is Los Angeles. But you can see it's not constant and some of them are larger than others.

I mean, yeah, if you're a small business, yeah, it's not going to take many gigs to take you offline. You don't need to send a 500-gig attack against most of the targets. Most of the DDoSes are smaller, but some of the big ones are very, very big. I mean, very big. Yes, like [Krebs] and a few others.

Let's talk about phishing. Who's been phished? Oh, you liars. You've all been phished. Our company phishes on purpose. They're evil. And I hope your companies do the same. Phishing is fraudulent practice of sending e-mails, trying to get you to go somewhere so they can steal your credentials. Or maybe so they can infect you so they can steal credentials, but it all comes down to the same thing.

Spearphishing. Have you heard the term spearphishing? It's just targeted. Imagine you're phishing with a rod and you're just

hoping any fish comes along. Spearphishing is "Oh, there's the fish I want, going to get him." So it'll be very directed to you.

Normally, when I see a regular phish, I will recognize it straight away because the generic… and I don't have a grandmother in Uzbekistan who's ill and needs me to send the money. They're just very generic. But when people start spearphishing you. Who's been spearphished? I wonder if you just don't know you got hacked. Okay.

So, if they start spearphishing you and they start doing things like social engineering and start learning stuff about you, reading your Facebook profiles, etc., it's much harder to detect. So that's what spearphishing is.

One of the ways they abuse the DNS is they use confusing domain names. We send e-mails out from icann.org. If we ask you to change your password on our systems from "Please change my password because I'm ICANN, really, really, I am, I promise, .com," it ain't us. We see people phishing registrants to try and get their credentials for their domain names all the time. We get complaints about this. It's another form of abuse against DNS. They register names that look like other names but they also target registrants to try and get their DNS credentials.

It goes up and down. You know sometimes we don't see many. Sometimes we'll see a few in a month. Strings with ICANN in

them and ICANN Compliance and dot something, dot TLD. We see them quite regularly. So, it's out there.

Here's one from berkeley.edu. I think they said this was the first of the U.S. tax phishes of this year. It's basically saying, "Hey, it's us. We're the payroll guys. Please log in to go and check your W-2." The W-2 in the USA is your payment statement for the year that you have to take to the taxman. If you want to get your tax early because you want to get that money back from the evil tax man, the moment you get your W-2, it's like, "Woohoo! I can go get my money." So, if somebody sees this and go, "Oh, W-2," and they click on it, they're probably owned.

This is a real phish. I see dozens of them every day in my mailbox. Unfortunately, just part of the world today. This one is a gov.co, so this is probably somebody's server that's being or somebody's system that's been hacked rather than something that's been registered for this. We see both.

A lot of the time these days, the phishers don't even bother to try and register because if they put ICANN dot blah, blah, blah dot org, most people will just look at the ICANN and they won't even read that it's blah, blah, blah dot org. Users are very easy to fool. They just look for the strings that they expect to see there and they ignore all the rest of it.

How do I learn more? Like I said, this is just an introduction about various types of abuse. Now, obviously, you can go to these sessions that I listed, and I recommend you do if you're interested. Some links here, as I said. We're going to put these slides up. The mit.edu explanation on malware is pretty straightforward and easy to read. I can also find you one that's really complex and looks like it's written in Martian, if you'd rather have one of those. A lot of these documents when they get really technical are confusing.

When people measure abuse, as this gentleman was asking about where is the abuse, a lot of the time, these lists are used for what they call block lists. So, lists that will, hopefully, protect you against malware.

Malware domains is a pretty good one. The ransomware tracker is a pretty good one. If you go to the SANS Institute, the Internet Storm Center, they actually have a suspicious domains list, which includes various lists, and is pretty good. But you can just go look at them. There's no danger to go and look at those lists. Just don't go to the names that they have on there. Don't try and see if you can actually get to any of them. They're not clickable.

Those are good resources to see just how rampant malware is and the kind of things that people are doing to try and protect.

Those sites also have other links about malware and teaching you about malware.

Botnet command and control. There's a really good paper from ENISA in Europe on botnet measurements and it also talks about DGAs, etc. And there's another one on the Usenet about how you actually track DGA botnets. There's been some really interesting work where you could actually just by looking at DNS patterns, you can actually work out algorithms and things. Some really, really smart, smart people working on some of these problems. So, that's a really good paper, too. That's a little bit technical.

If you want to go see that map, here's the link. It's very pretty. They update it every day. Every day, it looks pretty much the same to me. It's like, "Oh my God, it's a mess." But if you think it's a quiet day and if you want to go and see if it's a quiet day, that's a place to go.

Verisign, who a lot of you may know, is a registry, also have a little security group, and they do an interesting trends report quarterly. And then there's a lot of other people who do these, as well. A lot of distributed content providers will do this. Anybody who does a DDoS protection service do these kind of reports. There's a lot of information out there on the status of DDoS. None of them will make you happy.

If you want to know about phishing, my favorite place to go is the Anti-Phishing Working Group. That's a group of people that are tackling phishing. They also have a good report. The authors of that report, I believe, are both here this week, Rod Rasmussen and Greg Aaron. So, if you want to go and talk to them, this is a great time. Read the report and then go and ask them all good questions.

Also, PhishTank has some great data and they actually have lists of the latest reported names. So, if you want to see what name has been reported recently, it's right there.

That's a brief introduction. Now, there are dozens of other types of abuse that people consider DNS abuse, and I specifically didn't get into all of them because we'd be here for hours. So, I just want to open it up for any questions about DNS abuse, and I see one in the back. Thank you.

UNIDENTIFIED MALE: Thank you. Okay. My question is, is there any department in ICANN that is working with the various computer emergency response teams to handle these abuses? Because there's a lot of issues coming to the various [CERT] groups around the world.

JOHN CRAIN: This is specifically not an ICANN role. We are not a CERT. We are not any kind of security organization for handling these things. What ICANN does is we enable the setting of policy by the community. So, the mechanisms we have are through those policies fora. So, things like what we saw in the contracts.

Now, I run a small group called SSR, Security Stability and Resiliency, that we look externally at the identifier systems. So, when we see problems, we will tell people. We cooperate with a lot of people. We are a member of FIRST, which is the organization of incident response teams. For issues like Avalanche where there's a command and control that's going to affect a lot of registries, often law enforcement or the software companies will come to my team and what we will do is we will explain to them how the system works, how the industry works, and then bring them into touch with the right people.

And there's always this misconception that ICANN runs the DNS. We can barely run our own recursive resolvers. We do not run the DNS. We happen to run a few servers. We run some servers for .int. We happen to run a root server. So, we have DNS skills but we don't run the DNS any more than we run the Internet.

When you're dealing with actual operational issues, you have to get to the people who've got their fingers on the keyboard. So, if you want to do something that's at a registrar, you have to talk

to the registrar. If you want to do something that's in a registry, you have to talk at a registry.

What we like to say about our team a lot is that we work as introducers or trusted introducers. So, we work a lot with the operational security community. And if they have major issues, they come to us, but that's not what ICANN is there for. There are some people who think it should be and there are some people who think it absolutely should not be. And that, my friend, is a policy discussion and I'm just an engineer, so yeah.

But there are CERTs and there is FIRST, so there are organizations that deal with that, it's just not us. We do cooperate with them. Owen? He's going to ask an awkward question, I can tell, because I got people to throw tomatoes.

OWEN DELONG: [inaudible] specialize in awkward questions. Owen DeLong, Akamai. We're a registrar now. You talked about the policy being what ICANN can do and I agree, and I think that's what they should stick to because it's what they do somewhat okay job with. Last time I tried to poke my finger into policy, it was about trying to shove registrars and registries kicking and screaming into v6 and this was probably about 10 years ago, and ICANN politely told me, "Well, the contracts aren't up for renewal for a long time and so go away and bug us when the contracts are up

for renewal." And, of course, I did, but it seems to me that security and stability-related things, such as abuse that we're talking about. If we wanted to do something policy-oriented to attack them, might not want to wait for contract renewal to get implemented. Has ICANN considered putting provisions into the contracts that allow things like that to get addressed more rapidly?

JOHN CRAIN: Three things. First, I talked about people who do DDoS reports and being as Owen works for Akamai, I must give them a shout-out and say that they have an excellent one. As an engineer and a guy who wants all the badness to go away, I wish it was that easy. Policy is slow and horrible. It takes time. IPv6 is in contracts now for the new TLDs. We made sure it went in there as well as a lot of other things, and it is slow. Luckily, nobody's going to use IPv6 for the next 10 years anyway. It seems to be the slowest thing ever. I knew I'd catch you.

There are some things we've managed to do. For example, we have a process called the – oh God, I always get this acronym wrong – the Emergency Registry or the something Registry Expedited Response Process. What it basically means is if a registry wants to take action and our contracts or they believe our contracts stand in the way of them taking action, they can write to us and we can waive those clauses. And this gets used

all the time around botnet takedowns because, sometimes, for example, they have to register the names in a registrar that they set up, and some of the contracts don't allow that.

I am not aware of any case where a registry has come to us and said, "We want to do." They normally want two things. They want us not to tell them they're naught people for breaking the contract and they want not pay us for the names that they had to register because they [inaudible] and I'm not aware of a single case where we said no. And that process is slow, it takes at least a day, but there's also a clause in there. Normally, it will take three or four days, but there's a clause in there that also says that you can go ahead while this is going on.

We're actually thinking about how we go about revising that policy process to make it easier for the registries and the registrars because the registrars aren't mentioned in there. So, it might be useful for the registrars to also have such a policy. But that's got to come from the community, not from staff. It would be wonderful if we could write policy changes quickly, but that's not going to happen.

What we did instead and this came about because of Conficker 2010 is we put in a process whereby they can ask for leniency on the contracts. Because most registries and registrars want to do

the right thing and the trick is to allow them to do the right thing. Does that kind of answer your question?

OWEN DELONG: Kind of [inaudible].

JOHN CRAIN: We'll take the rest offline. Okay?

STEVE CONTE: Got one in the back here.

JOHN CRAIN: Okay.

UNIDENTIFIED MALE: Hi. Good afternoon. Just one question. I understood that in the context of Avalanche, one of the problems that emerged was that in a certain number of countries, there was no possibilities of taking action on domain names that had not been yet registered and that there was a legal impediment in that regard. Is there any recommendation or anything that should be said to encourage the different governments to enable action on domain names that are not yet registered when it is in

conditions of security like this or is it something that shouldn't be pushed because it has unintended consequences?

JOHN CRAIN: In not just Avalanche, but multiple – well, any botnet takedown, one of the problems you have is jurisdiction and differences in regulations. And in some specific countries, you cannot do anything to an asset, in this case a domain name, and I'm not a lawyer, by the way. I'm just an engineer. I'm just repeating what I've heard. So, if it's all wrong, blame the lawyers.

You cannot actually do anything legally to an asset that doesn't exist yet, so to speak. I think the agencies, because this is not an ICANN problem, this is a legal jurisdictional problem, I think they found ways around it.

If it's really problematic, there probably should be discussions about it, but I don't know where. I suspect not here. But there are lots of discussions around abuse that fall way outside ICANN's realm, as they should, discussions about treaties and the Budapest Convention.

We are a little, little piece of how people use the Internet. People forget that. They often think, "Oh, ICANN it's the one global Internet thing." But we're not. We're identifiers. We're mainly about names and we kind of touch on other identifiers.

What we can do is we can talk to these agents and give them factual data about how the system works and we can introduce them to people within the system. But when it comes down to these kind of discussions, I don't know where ICANN roles sit, and that might be a question for the Board or somebody like that, but it's certainly… Did I mention I'm just an engineer? It's certainly not for me. I think Dmitry had his hand up.

DMITRY KOHMANYUK: Yeah. I have difficulty understanding how an unregistered domain name can cause abuse. If a domain name is not registered, how does it get into the Internet and how does it resolve?

JOHN CRAIN: The specific problem here is related to DGAs, the domain generation algorithms. The infected machine has some code on it and it knows on which day it will ask a question to which domain name, which may not resolve today. But on the day that it wants to ask it, the bad guy will go and register that name and make it resolve, so now all of a sudden that name exists and they can get command and control. And that's why you have to prevent them from resolving on that day.

DMITRY KOHMANYUK: Unless the registry approves that name, that particular confusing string would not ever abuse. So, if there is a system whereby a registry looks for such irrelevant and arbitrary names and flags them as possibly suspicious names and blocks them from those names from ever being registered or even flags them for manual attention to see if it is probable that there is an authentic registrant behind the request to register, then such abuse could be [inaudible].

JOHN CRAIN: That's a lot of little moving parts that would all need to be worked out and would all have unintended consequences. So, although I agree with you in principle and there are people here that work at registries, so they understand much better than me all the problems that are caused by that – never mind the cost and the way what you do when you make mistakes. I think in a utopian world where you could absolutely know that this was going to be badness and stop it, maybe, but it doesn't work that way.

I know there are people who do variations of that to flag things but if it was that easy. And plus, then the bad guys are just going to start using names that don't match it. The bad guys will adopt. So, yeah. Interesting theoretical and I thought about that

myself, but I think in practice in the various registries, it's not that easy.

We've got a queue, so who's next, Steve?

Dmitry. [inaudible]. You should probably say your name, as well.

DMITRY KOHMANYUK: Sure. Dmitry Kohmanyuk, dot ua. Well, thanks for comments and while we can all sit [inaudible] we can do nothing, I can tell you what we did. Well, we did block Conficker back in the day and we have registry for TLD in Ukraine, which is half a million names big.

Well, yes, you can block all of DGAs in the world. There's so many people writing this every day. Plus it's stupid, right? It's like taking every shot of [every] medication you can possibly get sick from, you just overdose.

Going back to the domain operations, ICANN does operate a little bit and last time I checked they had 100-something nodes, and we hosted some and we still do. So, I would say people could do their part and I'm not selling you on ICANN service. Plus, you have to buy the computer yourself anyway. But you can increase the resiliency of the Internet domain infrastructure by hosting your own equipment and that's maybe not subject of this session, but I would just say the keyword is any cost and

another keyword is [inaudible] and I'm not going to explain what it is. You have to Google it and talk to me in private but also I want to say that ICANN to me is still a center of technical expertise, maybe not the biggest one, but it's open and community-funded. It's our money there. Remember, guys. It's not Google or Facebook.

The service that ICANN provides a free to use and they're free to corporate. Thanks.

JOHN CRAIN: Thanks and I didn't want to speak for you but I know there are many at registries that do everything they can to be able to work in these areas and I agree that taking down DGAs only goes so far because, like you said, there's new ones written every day and you see, even not the law enforcement capacities take them all down. So, they focus on the big ones.

TIMOTHY CHEN: Making me get your exercise. Thanks, John, for this presentation. Timothy Chen from DomainTools. One of the things that I see as an increasing number of companies that are broadly in the direction of Internet security are seeing value in the use of DNS data for things like threat intelligence and instant response work and more companies harvesting that data at

scale because you can do interesting things like show all the domain names that are resolving on an IP that may be bad.

As more companies do that and interrogate DNS over and over again, maybe move beyond just domains, which is a limited set host homes, much larger. Will that ever be considered abuse, do you think, at the ICANN level?

JOHN CRAIN: That's an interesting question and I don't know. So, you're talking about things like passive DNS and the way that we interrogate data. There's all kinds of issues with that around privacy, etc., and you'd have to ask a lawyer. I mean, I think if somebody – and this is hard because who isn't somebody here? If organizations are willingly giving up their DNS data, then maybe not, but then there's the end user issue and I actually don't know.

TIMOTHY CHEN: I'm sorry, the PII and the DNS data. What I'm trying to say was just the act of actually actively resolving. So, not passive what's happening and watching that and publishing that in some way, but saying, "Okay, if this data is useful, then I know all the domain names and all the host names out there." I'm just going to send a ton of DNS requests so I can always know let's say the

A record at a TTL and it's useful. Is that action, just that activity and using DNS, which seemed to be very small relative to the size of DNS but ever going to be seen as something that's not using for its intended purpose?

JOHN CRAIN: Haven't thought about that. That's a good question for offline. But there many – is it innovation or is it abuse? I don't know. I've not thought about it.

STEVE CONTE: Any other questions in the room? Kathy, any remote questions? [inaudible] from there, so.

UNIDENTIFIED MALE: Is there any other way by which a person who wants to cause abuse could cause abuse by not registering names, but actually by compromising a registry infrastructure over the registry backend infrastructure to place unregistered domain names as registered or even on a relatively local level, poison the cache server and place certain domain names to resolve and cause local abuse? Has any such thing happened?

JOHN CRAIN: There are all kinds of ways to do abuse. Luckily, most of the registries have very good security, etc. But like anything, if you can get to the data and change it, it's a form of abuse. And you can localize abuse, etc. Yes, of course.

We've seen publicly available information, we've seen registries have systems hacked and have to take action against that. It's just like any other system. A registry or a registrar or ICANN, we're all network operators. We're all vulnerable and we all have to take precautions.

GRACE MUTUNG'U: Thank you. Grace Mutung'u from Kenya. My question is there has been claims that sometimes government are using DNS attacks to shut down the Internet. I know sometimes this is not like an issue for ICANN. But I'm wondering from a technical perspective whether that is possible and if it is, where would be the right forum within ICANN to discuss that?

JOHN CRAIN: Shut down the Internet. The Internet. I'd hate to throw a challenge out to anybody by saying it's completely impossible, but I've not figured it out yet. The Internet isn't the Internet. It's a series of networks that interconnect, so you can take down parts of it. That's what DDoS does. You aim at a specific part. But

take down the Internet depends on for who. I can take down the Internet for your company by blocking your company but the Internet itself is still there for everybody else.

A system-wide catastrophic failure, there's a lot of resiliency built into the system, a lot of capacity. And knock on – I hope this is wood. We've never seen anything close to that yet.

Where would you talk about that in ICANN? As it relates to the identifiers, the things that ICANN's sort of involved in, I'd probably say one of the Advisory Committees, maybe. Maybe talk to some SSAC members. If you're interested in specifically against the DNS and the root servers, maybe talk to some of the… come to the RSSAC open session, the Root Server System Advisory Committee.

Like I said, knock on wood, we've not had that problem, yet. That's not a challenge.

UNIDENTIFIED FEMALE: Hi. My question is about registry basic agreement. I think that this anti-abuse of specification that it's only for gTLD registries. And what about ccTLD?

JOHN CRAIN: So, ccTLDs are considered – probably not the right word, but maybe sovereign. I'm not sure what the right word is but they are country-specific things and they generally do not have contracts with ICANN. However, they are heavily involved in ICANN policy discussions, so the ccNSO, etc. But they are normally local issues rather than global, even though they're globally visible. I don't foresee a time where they'd be contracted to ICANN because there's no need for that. Most of them work pretty well. But they have local regulations, local laws, local contracts in some cases, but it depends on where you are and which ccTLD.

If you have questions and you want to talk to a specific ccTLD, myself or a number of people here I'm sure could introduce you to them if you have questions. But it's not part of the ICANN contracting process. But they do participate in our policy fora.

STEVE CONTE: They're making me get my exercise.

JOHN CRAIN: Come on, Steve. Faster, faster.

STEVE CONTE: John, while I'm crossing the room, again, you're mentioning DNS. Does ICANN play any part or pay attention to any other unique identifier abuse that is relevant to the ICANN mission?

JOHN CRAIN: Well, yes. All the identifiers. I mean, you see most of the abuse in the DNS. That's where it's mostly visible. We've seen some interesting routing injection attacks. Those are interesting to. Hopefully, those won't take up where people are introducing IP addresses. But ICANN's not the main policy fora there. So, if you're talking about IP address allocations and how they're used, those happens in regional Internet registries and, in many ways, in the [nogs] and things where that gets discussed.

It's not really the prime subject here but we have the Address Supporting Organization that is here and they do work here. And we participate in the various RIR meetings, so yes, we're interested in it and we watch it. We're interested in any technological solutions to that, which there've been a few suggested. RPKI is the latest thing for authenticating routing. I don't know if it's the latest, but it's one of the big things, so we have an interest in that. But most of the abuse we see is normally associated with domain names but, of course, there's also IP addresses behind those and every other parameter that gets used.

[FABU]: In connection to phishing, it's actually pretty easy to have a name server create a name, create an e-mail there, something at apple.com, and sent to someone. And this person will receive it. It's very easy to phish someone like that. And I don't understand why this is still allowed.

JOHN CRAIN: Well, it's illegal.

[FABU]: I know it's illegal. It's illegal.

JOHN CRAIN: It's not allowed. There is no technical solution for that that I'm aware of apart from signing up for some of the blacklisting stuff and I don't think you want to blacklist apple.com. I don't know how you would prevent that from a policy standpoint because somebody is pretending to be Apple, apple.com. I can't see a policy solution for that because apple.com is a completely legitimate business doing completely legitimate thing, and they may not be on their machines.

So, there are lots of things in life that should not be allowed but they still happen.

[FABU]: Agreed but in the root, I know the DNS, I know all the [records] there. But not me, I'm saying the root. They know all the DNS records and, basically… Is it right? About the name servers.

JOHN CRAIN: No. That's not known in the root and there is a training on DNS basics and there's an RSSAC discussion next, but the root servers don't see all the DNS traffic. They don't know. It's a distributed hierarchical system. I operate one of those root servers. We actually see very little of the traffic. I don't see a policy solution and, frankly, I don't really see a technical solution, either, that will work on a global scale for that. Because if there was, we will have probably found it by now.

Bad people will do bad things and they will find ways to abuse you and that way of pretending to be a different e-mail, you can do that. I don't know. Maybe you'd have to change the mail protocol. I don't know what you'd have to do to fix that one. But it's certainly not something that I think policy is going to help.

STEVE CONTE: Just taking that as an opportunity to do a selfish plug for the how it works sessions. Next session at 5:00 in about 30 minutes in this room will be the Root Server System Advisory Committee.

They will be talking about how the root operates. They will be discussing some of the concepts of that and then what their role as a root server operator is.

And then whether tomorrow at 5:00 and I think it's this room but it might not be. We have another repeat session of DNS Fundamentals. It talks about just general how resolution takes place on the Internet, too. I invite you to come to either or both of those, as well.

Any other questions? Kathy, last chance online. Anything?

KATHY: We're still cool. Nothing.

STEVE CONTE: John. I want to thank you, then, for spending time [inaudible].

JOHN CRAIN: Thank you, everybody. I'll be around. Any easy questions, come find me. Any hard questions, find Steve. He knows all the answers, too. And thank you very much. Thank you for your time.

STEVE CONTE: Please join us in 30 minutes for RSSAC's presentation.

[END OF TRANSCRIPTION]