UNKNOWN SPEAKER: Okay.

TERRI AGNEW: Good morning, good afternoon, and good evening. Welcome to the At-Large Capacity Building Program 2016 the ninth webinar on topic Current Security Trends Impacting Registrants and End Users taking place on Wednesday the 19th of October, 2016 at 21:00 UTC.

We will not be doing a roll call as it is a webinar. But if I could please remind everyone on the phone bridge as well as computers to mute their speakers and microphones as well as state your name when speaking not only for transcription purposes but to allow interpreters to identify you on the other language channel. We have English, Spanish, and French interpretation.

Thank you for joining. I'll now turn it back over to our moderator Tijani Ben Jemaa, Chair of the Capacity Building Working Group. Please begin.

TIJANI BEN JEMAA: Thank you very much, Terri. Good morning, good afternoon, and good evening. This is the ninth webinar of this year of 2016 for the Capacity Building Working Group. So, today we will speak about the current security trends impacting registrants and end users. This topic has been chosen by our specialist in security, Julie Hammer, who is also our liaison with SSAC.

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.

And so, first I will give the floor to the staff for some housekeeping, and then we'll come back. Staff please.

TERRI AGNEW: Thank you, Tijani, and this is Terri again speaking. Just a few housekeeping items before we begin. If you would like to ask a question during today's webinar, we do have the question and answer pod now located in the lower left-hand corner of your Adobe Connect. Please type in your question there and we'll have our presenters or somebody answer the question for you. Also, after today's presentation we'll have a quick pop-quiz question, and at the very end we do hope that you stick around for some evaluation questions. And we have seven evaluation questions.

For the pop quiz and evaluation question, the polling pod at that time will appear in your bottom right-hand corner of your screen. I would also like to remind all participants, if not already done so if you could please complete the At-Large survey.

As many of you know, the At-Large Community is going through an independent review. And all of you are encouraged to participate in the global survey, which is available in English, Spanish, and French. Your feedback would be extremely valuable to improve the organization effectiveness of the At-large community. You can click on the links of the web links pod to access the survey in the bottom right-hand corner at this time.

With this, I'll now introduce Julie. Please begin.

JULIE HAMMER: Yes. Thanks very much, Terri. It's a real pleasure to introduce Rod Rasmussen to you this morning. Rod is Vice President of Cyber Security at Infoblox. And he's a widely recognized leading expert on the abuse of the domain name system by criminals. Rob cofounded and led the technical side of IID, a cyber security company focused on cyber incident response and information sharing which was purchased by Infoblox earlier this year.

Rod has also been a highly active participant often in leadership roles in industry and in other global organizations addressing many of the cyber security issues at bay. Rob's the co-Chair of the Anti-Phishing Working Group's Internet Policy Committee, and services the APWG industry liaison. In this role he works closely with ICANN, the International oversight body for domain names as you all well know. And he's a member of SSAC and a very active member.

Rod is also a member of the Online Trust Alliance's steering committee and a member of the FCC's Communications, Security, Reliability and Interoperability Council. He's an active participant in the Messaging Malware Mobile Anti-Abuse Working Group, and he's IID's Forum of Incident Response and Security Teams first representative. Huge number of international roles there.

Rod's a regular participant in DNS-OARC meetings and that is the World Wide Organization for major DNS operators, registries, and interested parties. So, you can see Rod's got incredibly appropriate credentials to

be talking on this topic, and that's my great pleasure to introduce him. Thanks very much, Rod.

ROD RASMUSSEN: Well, thank you, Julie, and thank you to everybody on the call today. I appreciate your time and this opportunity to bring you up to speed on many of the issues of the day when it comes in particular to the DNS. And you said it is seeing and receiving in and part of as it is an area obviously near and dear to our hearts here in the ICANN space. So, I will without further ado move through here. And hopefully these slide - I do have the [unintelligible] I do. Here we go. All right.

So, I want to basically take this time to focus on DNS. I know the topic was rather broad, and I could spend a lot of time talking about many of the cyber security things that are going out there that could affect you. In fact, I'm under the conference in Sydney right now where many of these items would be discussed today even. But many of the primary things that you may be hearing about in the news or should be aware of do involve DNS as part of the equation as DNS as you know from, you know, kind of standard Internet operations is a basic part of almost everything you do on the Internet whether it's your e-mail or your web browsing or on any other kind of communications you're doing on the internet. At some point it touches on DNS.

So, we're going to talk about what those things are, where that is showing up within the DNS ecosystem. That's where the role of ICANN comes into play at least to some extent with the provisioning of DNS being done via registries and registrars which are obviously within

ICANN's purview and then talk about some of the things that we might do dealing with these issues both [in] how do I protect myself and my business or my organization or just, you know, people I care about from these issues. And then some of the things we might want consider at least having questions about central policy implications and the like and the environment we're all working on will begin within the ICANN community. That's the agenda for today, and I will see here – here we go. Oh, that's a little about me, but Julie already did a very good job, a thorough job covering that.

So, let me see. Let me get into the various threats. And I know many of you on the call, and I know many of us have met at ICANN meetings in the past and typically at those meetings there's – when you go to a session to talk about abuse it often gets into the nuts and bolts of how the registrar registry community's involved, what is going on with particular areas. I thought it would be good for this thing to kind of step back and take a look at what are the actual threats? How do they actually impact people at organizations? So speaking to the details of that so you understand them when it comes to the net effect, when it reaches our meetings in discussions within the ICANN world what that effect really is, because like any field, there's a lot of information that the people who deal with it on a day-to-day basis know, and you're having conversations around policy or activities of there's an assumption of [inaudible] knowledge which just isn't there. That, you know, as I said, that could be in any field. This is definitely one of those.

But I want to divide this up into three areas of attacker or issues around the DNS. The first is tax upon the DNS infrastructure itself. And that is using the DNS like against victims kind of directly. Then there's use of

DNS as it should be used in general which is as an infrastructure component or a naming protocol. And bad guys use DNS just like the good guys do and want to make sure that the infrastructure that their using is resilient, is easily reached and things like that. So, I'll talk about how the DNS is used as part of these things as is with any normal kind of Internet service, if you will.

And finally, I want to talk a little bit about the DNS being used as an attack vector itself in unintended ways in particular as a way of moving data that is not the way in DNS was intended at all, but it is a very effective tool. And we'll get into that here in a little bit.

So, let's talk about the targets and the motivations and why we're seeing various things.

TERRI AGNEW: Excuse me. This is Terri from staff. I apologize for interrupting you. Is it possible to adjust your mic a little bit? Our interpreters are just having a little bit of difficulty picking up everything that's being said. To them you're coming across a little muffled.

ROD RASMUSSEN: Okay. Is this better?

TERRI AGNEW: Do you mind just saying a sentence?

ROD RASMUSSEN: Okay. Well, I'm going to be talking about tax on DNS services and operations – is this slide. That better?

TERRI AGNEW: Not yet. Could we ask if you could move your mic just a little bit farther away from speaking?

ROD RASMUSSEN: All right. And I'm trying it again. Is this better? I'm trying a different approach.

TERRI AGNEW: And it came across clear, however, just not loud enough now. I do apologize.

ROD RASMUSSEN: Yes. I'm not sure. That was forming an echo it sounded like with that. This better now?

TERRI AGNEW: And I'm just waiting for confirmation from our interpreters. Thank you for adjusting. One moment.

TIJANI BEN JEMAA: Really, it's too loud for me. He's really loud. [Inaudible].

TERRI AGNEW: And, Rod, unfortunately the adjustments are not working the best. Do you have a number – a telephone number we could perhaps dial out to you on?

ROD RASMUSSEN: Okay. Yes. Just a second here. Actually, I think I can throw out myself here, can't I?

TERRI AGNEW: I'm sorry, can you dial in yourself? You certainly can.

ROD RASMUSSEN: Yes. [Inaudible] so I'm the Australian number if there is one.

TERRI AGNEW: Certainly. Let me try to quickly get that up for you. One moment.

ROD RASMUSSEN: Yes. This is odd if it's loud for some and interpreters can't hear it. I don't know if that's on my end.

TERRI AGNEW: I do apologize. And, Rod, in the Adobe Connect chat pod at the bottom I did put – oh, you said Australia, correct?

CHERYL LANGDON-ORR: His memory show 1-800-009-860. It's been a long time since I've had to use it.

TERRI AGNEW: I did put two phone numbers in the Adobe Connect pod for you. Is that okay?

UNKNOWN SPEAKER: Yes. [Inaudible].

TERRI AGNEW: [inaudible]

CHERYL LANGDON-ORR: That's correct. Yes. Well, Julie, I'd be surprised if I'd forgotten something like that out.

TERRI AGNEW: And thank you, everyone, for your patience while I readjust this. And we do apologize for the interruption.

ROD RASMUSSEN: All right. That's not working. Let me give you my number to call. Let me know when you're ready.

TERRI AGNEW: I'm ready.

ROD RASMUSSEN: Okay. So, country code 1-253-297-0377.

TERRI AGNEW: Okay. One moment please. And the operator's dialing out to you right now.

ROD RASMUSSEN: Hello.

TERRI AGNEW: Hi, Rod. It's Terri. Thank you for joining on the [inaudible] telephone. And this is a reminder to turn down your computer speakers.

ROD RASMUSSEN: Yes. I just did. So, is this working better for the interpreters now?

TERRI AGNEW: And I'm just checking with them. One moment please.

ROD RASMUSSEN: Okay. Yes.

TERRI AGNEW: Much better. Again, we appreciate this, and apologies for the delay. Please proceed.

ROD RASMUSSEN: Okay. All right. All right. Well, even the operator told me I was coming in fine before. So, it sounds like a vagary of Adobe. Okay. After that let's move on here. So, the idea here is we just talking about the various things that can happen to your DNS and why things might happen like this. So, kind of very traditional things around taking out your service, so attacking your DNS infrastructure with DDoS attacks or using actually your DDoS attacks using your DNS to reflect DDoS off of your infrastructure and to hit other people with it. And that obviously is not a thing you want to have happening with your DNS. That leads to potential people blocking your DNS and things like that. There's also trying to break in and hijack it or some snooping, the kinds of things at you when you're making DNS queries.

Those are kinds of things, by the way, DNSSEC helps you with if you were wondering what DNSSEC [is] for. It's exactly that kind of thing. And so those people trying to send you the wrong information when you're looking up a particular resource using the DNS. And then, as in the traditional kind of computer intrusion looking for vulnerabilities break in and then doing a lot of things with reconnaissance, being able to take a look at things which are within the realm of DNS. And I've kind of extended that a little bit here to include who has information, yes, that's tied to the DNS and pretty much every – at least all the GTLDs. And that reconnaissance could mean that people are trying to figure out who to spam or who they might want to send a phishing attack to very

personally, not particularly a reflex on when people are setting up to do an attack to try and gain access to your domain name through your registrar. That's a fairly – unfortunately a common case these days, you know. I'll explain that more here in a little bit.

That's just a quick section on how people can attack you through the DNS or at your DNS that you have set up for domains that you own or manage. But the main thing is the DNS enables you a flurry of the greatest contents and services whether it's the web or e-mail or other kind of activity like Adobe Connect I would guess, all the various services that are over there. So, this kind of activity ranges from kind of your unwanted offers and kind of spammy stuff and things that are maybe illegal in some jurisdictions and illegal in others and people try to beat around that to real criminal activities. They are trying to steal money, and data, and valuable assets. And of course some of the things we know that state actors are doing to try and in particular that's usually around data theft and that almost always involve DNS at some part of that activity. And I already mentioned why people would want to use that, so the same reason that everybody wants to use DNS in the first place, why it's such a great thing. Unfortunately, it's a great thing for the bad guys too.

So, just going to dig into some of the techniques here a little bit more so you get a better understanding of that a lot. And when we see the in kind of large-scale operations to register, I've got marked dodgy domains here, suspicious, malicious, whatever you want to call them. I call it dodgy because it depends on the jurisdiction as to how what are legal, or illegal, or grey. But one of the biggest drivers of these kinds of registrations is around neighboring e-mail campaigns, getting [invasion]

techniques in order to fool services that rely on reputation of a domain in order to make decisions about how to treat it.

So, whether that's lifting something higher or lower in search engine rankings, or whether or not to deliver e-mail based on the fact that we've seen spam from a domain before or not or whether or not to allow something like a Bitly type service for web forwarding. What I actually do with that – they – one of the drivers of large scale registrations of these things is that fact that they develop – these kinds of services develop a reputation for domain names and then we'll either gray or blacklist them for their activities.

So, that drives the bad actors to since you have to continually get new resources. That means going out and registering your domain names, or at least getting new DNS resources. Some of the things that drive activities in one – let's say a registrar in one country versus – or one area of the world versus others is that if I set up a domain name monthly I'm pushing pharmacy into the United States, well, there's laws around that in United States and you have cooperation between other countries on that. But there's other countries where doing those kind of things, you know, there's nothing wrong that, at least there's nothing wrong legally. And so, if I, you know, had my registration in a different legal jurisdiction then it's much harder for somebody in that other [inaudible] kind of victim once you put a jurisdiction to get something done because there's no local law where the registrar or the registry is effecting that. So, that kind of shows right there the problems we have.

And we've all been dealing with these for a very long time. And I know there's a lot of work on this, but it's an undissolved problem. It's a

personally mitigated problem, but there's an unsolved problem where we have this conflict between local law and the fact that you have global resources that you can get them in one legal jurisdiction and use them and basically globally. So, I think that's a good example of why people will go to one full place or another for getting their DNS resources. Excuse me.

So, moving on to more fun stuff that is in my bailiwick, fun and un-fun I guess, is the use of malware use of the DNS. And the data is 91% is kind of the number that people have been using for a while. It's probably more close to 99% these days. But there's been solid numbers there. But what has [inaudible] use DNS the main purpose is to establish an [under-control] channel. So, a highly effective computer, it needs to reach out for instructions from a central resource to tell it what to do, whether that's to launch a DDoS attack or to take data off the network or to do traffic redirection if I'm trying to, you know, like hijack somebody's browser session and redirect it somewhere else.

Those are the kinds of the things that are being done. And it's all that control is being done over the DNS because I want to have a resource that is not easily blocked by a firewall. So, if I try to hard-code that to an IP address that I might own those kind of activities are usually seen and much more easily mitigated by controlling the IP address. So, and it allows me to move those resourcing around and there's some other techniques that we'll talk about here in a second.

But the despite that, the irony of that is that in today's world, very few organizations are actually looking at what's going on with their DNS to look for these kind of activities. We're starting to see more and more

people do this. But it's put a big hole in the security world for many years. And then obviously I've got a couple of facts and figures there about why this is important. There's a lot of laws and some things like that which we've all heard about. These are things on the news. And they can often be difficult to report and mitigate where those service providers are providing these domain names.

I think the best example that hopefully you have heard of at this point is the phenomena ransomware. This is a particular type of malware. But it has been [inaudible] the story of 2016. And it's an example where DNS is used in all of the stages of a crime. But the idea of ransomware is that I'm going to encrypt – I'm going to get that malware onto your computer after having figured out where you are and getting you infected. There's lot of different ways to get you infected whether that's clicking on a link, clinking on an attached e-mail, or e-mail attachment, things like that. After I've done that, I'm going to encrypt your disk, the files on your disk. And then I'm going to deny access to that and probably just give you a little message saying, "Hey, you've been hacked. Contact this e-mail address for instructions." And then those instructions will be able to [take] finance to get your files unlocked. So, it's really just holding your data hostage. And actually in most cases criminals will give you the key to unlock your data once you actually pay them [inaudible].

The scary thing about this is the bad guys have learned how to target – based on the victim they have, they've learned to target small, medium business and professionals like accountants and lawyers who have very sensitive data on their computer are thus more willing to pay a higher ransom. And that has gone from what was about a $50 million problem

– maybe a little bit bigger than that worldwide – it looks like it's going to be on pace to be well over a billion dollars' worth of ransom paid. And that's not even counting the losses based on people having their data permanently gone.

So, it's a very fast-growing phenomenon. And so everybody should be aware of. And there's a real lack of awareness still out there. Some recent surveys showed about 50% to 60% of employees and organizations were unaware that this is going on. So, it's a very scary and active thing that you should be aware of. And unfortunately, we have leverages of DNS are almost every aspect of this operation even right down to the registered domain names so that they have a place that you go easily putting your Bitcoin information to pay with a handy-dandy site for doing that.

So, let's talk about phishing. Still very popular. There's a vault moving away from traditional – what you would think of traditionally as financial services, things like that, more [inaudible] retail online services where they're trying to get credentials. And there's some figures there around the cost. For a major target of phishing on an annual basis it's a pretty proposition as you might imagine. But the effect on the users is shifting. It used to be you didn't have much liability depending on your jurisdiction. Now, it's their using your access credentials to get in the services you use to then turn around and do other criminal activity with typically.

So, that's something to be aware of and how that's going. Spear phishing which you may have heard of is really targeted phishing where they're going after particular individuals or at least types of individuals.

Sometimes it's masked spear phishing when they're going after people of a certain demographic and see – so they cast a little bit wider net. But what's of equal importance there is something we call business e-mail compromise or CEO scams where their intent here is to get a hold of – get access to the e-mail system typically that is used by a CEO or president, or high-ranking officer of a company, and then use that account to then send e-mail to somebody who controls the finances. And the message will say something like, "Hey, I'm on a plane, or plane's about to take off, we need to transfer $100,000.00 to this vendor, and here's the account information." And then they'll follow-up and say, "Hey, I really didn't know this has happened." And then there's a large amount of this going on. Unfortunately, those kind of losses are typically not covered. So, this has really impacted a lot of businesses to the point of even bankruptcies and the like.

And other variations on them could be I could register a look-a-like domain name to your business organization and send an e-mail from that. Another problem is that there's a lack of [inaudible] in place for your actual domain. So, I can send it. It looks like the from address is from a domain that could be [inaudible] but the [inaudible] replied to. Or if I compromise the account, I may or not be able to send directly from it or not. Sometimes you can't because they'll [spook]. So, those are all factors there.

Just some statistics from the first quarter, first half of this year. And these are from sites reported the EPWG. And you can see, it isn't going away. It's actually gone up a fair amount. We haven't really changed the reporting observations there, so there's not really a bias. That's a true growth over that year so far. Excuse me.

And this next slide is the – that's the latest quarter of data we have what the targets are. You can see in the orange there is financial and grey is payment. That's about a third, not even that silver quarter of targeting. And the rest of it is non – what you would think. You think that typically phishing is banks. It's definitely not just banks. A lot of the services are like coming at iTunes and things like that where people are trying to break into accounts like that instead of banks.

And one of the problems I mentioned already is the DNS [inaudible] monitored. And one of the reasons that it's very effective as an attack is it's a have-to-have service. It's got to work. It's got to be ubiquitous around the network. So, you don't usually see it as a traditional threat factor. And that leads to the ability to basically trick people and use the DNS in a way that is not intended for things like transporting data, signaling data off of networks, excuse me – tunneling [inaudible] and setting up like a VPM. And I'm going to explain how that works in a little bit. This kind of data exfiltration or say more of it latest point-of-sale malware, for example point-of-sale being the little, you know, the readers of your credit card at a retailer, the latest one uses this kind of technique where they're actually using the DNS to transfer the credit card data out to the bad guys off the network. And it's just not getting picked up by your traditional security tools, which is a really troubling kind of development. And it's been a tool traditionally more of a kind of state actors and espionage. Now, it's becoming part of the kind of standard cybercriminal toolbox.

So, that's been kind of the crimes and abuses that are going on. Let me talk a little bit more in-depth on the techniques, how are people doing it.

So, obviously one of the easiest ways to use DNS, the infrastructure is get a domain name. And we all know how to do that. But when criminals are doing it, they're typically doing it with stolen credentials or using like a stolen PayPal, or a compromised PayPal account, something like that. You have somebody that's using a Bitcoin and some of these cryptocurrencies and things like that, which are anonymous. Free is always good.

And we definitely see a correlation between domain price and criminal activity because bad guys have credit limits even if they have stolen off somebody's credit card, they can get more resources with the lower the price. And free is often not even a check, right, on whether or not that's a real of kind of credential because, hey, you're just giving it away. And then of course even compromise and account that somebody has and use like a credit card that's attached to that. And then we see resellers that are not really resellers. They're signing up as resellers of domain names or registrars but they're really part of a criminal enterprise of some sort.

And of course you can just steal the names. You can compromise a website and add your stuff to it. That's kind of traditional hacking [inaudible]. You can also compromise the DNS operator. That's kind of rare, but we do see it where people are able to break into the services providing DNS. It's typically and ISP kind of situation. And that's usually because somebody's used a really weak password or their password was stolen somewhere else and it was reused. Because if they used the same password in multiple places that's very common. That's also the same with the registrar account. You can break in [inaudible] account at somebody's registrar that manages their domain name because they

use that same password with another service that was breached, or they have malware on the computer and the bad guys got that information from them. So, we very rarely see, which is good, [tax] directly at registrar's registries to try and take things over. That is a very rare thing still. So, that's the good news then.

I'm getting some music. Some lovely music.

TERRI AGNEW: And this is Terri. We're isolating the line now. It'll be just a moment for us to find it. No apologies.

ROB RASMUSSEN: No worries. Yes. I think that is Chopin. All right. So, this nice little graphic here is a nice – describes the spear phishing which I've already described, so that's a nice little kind of graphic to explain the whole thing. And because I've had these delays I'm going to move through this pretty quick and [inaudible] we have time for questions and all that.

So, I want to talk about a couple of the techniques that are used within the DNS that are interesting, that are unique. Let me show you what the value it. Now, the first one is fast flux, which we even had back in I don't know, 8 years ago. We had a vast flux policy discussions and you would not believe some resolutions and policy actually created about that. The idea of it and still around is that I've got a resource – I've got a network of computers that I've got compromised, my bots. And I want to redirect a domain name to them, and this getting around firewalls and IP reputation basically. And so, I'm going to flux or change rapidly using

the DNS, the A records that that domain name points at. And that allows me to keep the domain up for a long time even if bots are being blocked or things shut down or in the way. And I can also flux the name servers, so I can change name servers if people are trying to block my name servers or going after that resource, I mean I can also flux multiples at a time. And this gets around several different techniques, at least it used to be around. That would be kind of static protection mechanisms.

The problem with fast flux is this is what your content delivery networks use as well, so things like [inaudible] CloudPlayer use the same basic technique are using it for content delivery, load balancing, local delivery of, you'll type in a domain name and [inaudible] get an IP that's closest to you, so that you have the lowest latency, so it returns the page fast, right? So, they look just the same pretty much because there's some little differences between them which are important to know. I think I have. Here's what an attack looks like. We'll just take it through this real quick.

You know, I already explained, you got your bots. I'm going to set up a phishing [inaudible] and I'm going to set that up on those bots. And I'm going to get a domain name registered. And I'm going to change the A records rapidly so it's always pointing at something new all the time. Then I'll load that bonus website basically onto that. And then I'll fire out my e-mail has link to the domain name, and the customer as a victim go to that and it doesn't matter what the particular bot they get. I have backend control of that. And I just keep repeating that. So, that's how fast flux kind of works in the background. And I have a little bit of map. There's no door. There's no pop quiz on the map. But with interest

there's a whole bunch of ways that you can now detect this kind of stuff and not hit false positives by looking in our content delivery network. So, you could actually find this stuff. And that's fast flux. That's pretty straightforward.

Domain generation algorithm, they are… This one is resources, so that if you think about if I have a command and control for a malware, if I reverse the malware or it's been detected for a long enough time I can go out and get that domain shut down or I can block that various ways, so I can protect myself from that in theory and back to in practice. So, what's happened, and this is kind of state of the art. Most of the malware today is they use a domain generation algorithm. What that does is there's a mathematical routine gets built into the malware and it generates a list of domains pseudo randomly but there's actually a formula that is based on the other day of the week, or the date. And then it creates this kind of random looking, typically a random looking domain name. And the malware will try and reach out to its list of generated domains and try and find its command and control server.

That allows you to be resilient over time and provides headaches to those of trying to shut this stuff down, because if we could think about it there's just one domain to go get taken care of that's pretty easy. If there's a whole list of them that change every day that becomes hard. So, the good news about this though is that if you're monitoring our network for DNS, you could actually see these things because an unaffected machine will reach out to domain that doesn't exist and they'll do it in burst. So, like every hour on the hour they'll reach out for a whole bunch of domain names that look weird and don't exist. So, you can find it if you're looking.

Also, if you get the malware you can actually reverse engineer that algorithm, and then you can know for sure what the next domain's going to be, or next set of domain's going to be. And just sort of some history and the start of 2008 and I know a couple of you have heard of Conficker. That was the big one that involved a whole big effort that ICANN actually coordinated or have coordinated around trying to shut down the ability to register these things. And when Conficker started out, I believe the list was 500 domains a day. And once that successful effort, we're at the Conficker Working Group, we put together this great group of registries and we're locking this stuff. The bad guys says, "Oh, well. That's nice. Here's 250,000 a day to try and block." So, that became, as you might imagine, a really hard thing to do. We actually did do that for awhile. All of them were being blocked and Conficker got so much press. [Inaudible] anything with it. But that made it really popular for malware [inaudible] to use. So, it's used to this day as the standard, the gold standard for how you do this stuff.

So, we've got hundreds and hundreds of different DTAs out there for different forms of malware. And then, if malware's sold as a kit you actually as a bad guy you pick your own random seed and that's added to the thing. So, even with the same malware you have different DTAs being used based on who's actually running them, so there's a lot of random looking domain names being generated.

The good news is there's been a ton of research done on it. Since then there's a great amount of industry sharing as to what those algorithms look like, what they generate. So, we've got a pretty good idea on what they after they've been established a while. But every time something

new comes in which is every day you don't know what it is. And this slide here shows what those kind of domains look like.

As you can see those are not things that human beings would typically register and use. They are very easy to see once you've got it. They even look like they're encrypted which actually is, so there's all these techniques for finding that kind of stuff through machine running and things like that. So, what's happened is some of the malware authors said, "Oh, well this is a problem. It's too easy to find our stuff. So, what we're going to do is use dictionaries and we're going to use real words and we'll create an algorithm to combine real words."

So, this slide here is talking about something a case study CrowdStrike worked on. There's a link to it in there. But here's the dictionary that's being used. And what's happening is that the malware is taking two words from that dictionary. If we're using an algorithm and putting them together now they've got nets at the end of them. It creates its list from that. So, those are often, I think the – I'll flip back a slide here. The bottom point here is really important. This is really bad if you own a domain name that happens to coincide with one of these DTAs that gets generated that day. Because what'll happen is all those bots, and if it's a big bot that will reach out to you and try to get commands from your web server, your mail server, whatever it is. And that may actually be a DDoS attack on you.

You'll be off the Internet for a day while all these bots are reaching out to you for non-inclusive commands. And then as a result you might have your domain blacklisted as well, which is obviously not going to be a lingering problem. So, these kind of DTAs out there, even if you're not

worried about the malware they can come and effect you because they have basically a collision with your own domain name. So, that's a problem.

The best way to find the DTAs are I mentioned reverse malware and then machine learning analysis can help you find these things. Because as you might imagine there's the techniques involved would find those kind of patterns very easily.

And here's a little bit of machine learning stuff for you real geeks out there and the various facets we use. I'm not going to go into the math here. Again, I didn't promise no math. I promise I won't make you learn the math, because I don't even know all this stuff. The smart machine learning guys know how to do this.

That takes me to the data infiltration. Cool. So, the idea here with data exfiltration over DNS is that I've got an effected machine, and I have file on that. And I want to get that - or sensitive information. I want to get that out of the network undetected. So, my infected endpoint I've got this malware, and it says okay, great. I am going to take that data, you know, you could see some examples here that are in plain text. Domain, social security number, date of birth, all licensing information, whatever I want. I'm going to then make those DNS queries. I'm going to say here's… I want to look up Mary Smith dot [inaudible] dot com. And that's going to go to a DNS server. DNS servers going to go, "Ooh, I don't know where that is. It's going to go right out to the world through all the forwarding or whatever you have set up." And that question will get asked to the name server for [inaudible].com, which means if I'm the bad guy and I'm running that name server every time a query comes in

that piece of data I get a hold of. And I can even if I'm running that name server respond back with and answer.

And it's also something that says like, "Oh, go steal John Smith data and give that to me," because I can respond back with an A record that's also got some information or an IP address that in the [inaudible] IP you actually you would have an encryption technique to know that this IP address means do this. And you can also do this with text records very easily. So, I request a text record and it passes all that.

So, this is a really effective way of exfiltrating data without anybody knowing about it. So, you really have to be watching your DNS in order to find this kind of stuff and looking for interesting bits within the DNS queries. And this was originally done by state actors. This was done by the phone service or the intelligence services. Now, it's being done by just standard malware authors.

The last one of these I wanted to cover was something that's really new and really something to be aware of as a domain holder, domain owner. And that's a technique called domain shadowing. And that is in the last 18 months or so – this is really taking off. It's been around a long time. We've seen people do it, you know, 10, 15 years ago. But it's become a much more commoditized. Some people, again, criminals these days are being very specialized. They'll develop kits, or software packages, or services and they'll offer those up to other people who want to actually do the crime. They're just providing infrastructure, and this is a great example of it.

So, what they do in order to get around the fact that they're looking at domain reputation, which, you know, we talked about your spam and things earlier is they'll abuse a good domain's reputation. But instead of kind of traditionally when somebody's taken over a domain, they do something to that domain and deface it or they turn it into a phishing site and do something to it. No, that's not what they're doing now. What they're doing now with this is they'll break in to the – it'll usually be the registrar and the registrar that had to provide your DNS service or that's got a nice automated control panel too because that makes it easier for them. What they'll do is they'll add a whole bunch of new host names to that domain name. So, it could be fubar.goodguy.com. And they'll www.goodguy.com alone. And so nobody's suspicious of anything. But in the meantime those other records are being used for criminal purposes. So, they basically, they don't have to register a domain, they just add subdomains to an existing food reputation domain. And a lot of services are setup that the reputation is at the domain level not at the host name level. This gets around a whole bunch of different schemes out there. And as you might be getting the theme here is there's measures, countermeasures and we have this cat and mouse game all the time. What this is particularly being used for right now is this thing called an exploit chip. An exploit is again is this commoditization of the criminal underground. And what that is, is there's these kits. They are kept up-to-date all the time with the latest vulnerabilities browser. And people are breaking the websites or set up new websites on their own even [inaudible] things we've already talked about. And those sites will have, if you visit them, they will actually fire off his exploit kit. And it will figure out what kind of browser you have

and then attempt at the list of known exploits against your browser until it can break into your computer. And it's just visiting it.

And this is really, this is why you don't click on links even if you know they're bad, right? Some people he just can't help it. They're like "Oh, I know that's a phish. I'm going to go take a look at it. [inaudible] that site is." Well, they might have that exploit kit on there and then your computer's been honed at that point. So, that's domain shadowing.

Domain shadowing is a tough one because the machine analysis, soon as they find them you have to really do this kind of as an almost a decision tree kind of thing to figure out where they are. So, you do things like look at the zone files, look at new things coming in long existing domains that just don't make sense. But, again, content delivery networks and various advertising networks use these same kind of techniques or false positives their problem. And then even if you do find these things, if you're dealing with it you want to obviously notify the person whose domain name has been, the domain registrar account's been broken into. But from a kind of a mitigation standpoint you don't want to block things that are typically small to medium sized business and people want to actually get to those sites. You don't want to block those. You just want to get the bad guys are using. And that's typically hard. People don't have their things configured that way.

All right. So, that's all the problems. Let's talk about where we're seeing that in the ICANN World. All right. So, there's a couple of organizations that I'm sure you've probably heard of Spamhaus is one that shows up at ICANN meetings fairly regularly. Given the name if you are unfamiliar with them they are, they're the world's leading have authority on spam

and dealing with it. And a lot of ISP subscribe to their list for keeping best of [inaudible] networks. So, Spamhaus provides a couple of different lists particularly for our communities. We can actually go see this stuff as to what are the top ten current registries and registrars that you're having problems. Registries at the TLD level at least.

And to be fair to things like .com where your half of domains in the world or just about are .coms. And as you might imagine, there's a lot of problems in .com. So, what they've done is created this formula that normalizes for the size of the domain or the entire domain's out there. And when I say out there, when Spamhaus's methodology, and I'm going to show you the list in a second. Their methodology, what they do is they take a look at the mains they're seeing. And they have visibility into a couple different places – three or four different places. One obviously is e-mail basically going through. So, they're seeing any domains that are still appearing in e-mail. They're seeing domains being used in the DNS because they have a passive DNS replication. Passive DNS replication is basically taking and adding an observation point to multiple main servers out there that are resolving things like at ISPs or universities, or enterprises and just looking at the outbound query and the response. It's the public Internet side of the request. They don't look at the internal side. They don't know who's asking the questions or things like that. What they do know is what's being asked and what's coming back. And then that gives them an idea of what domains are actually in use.

So, they take the ones that have been classified as being bad and by that number they used, they're actually using and multiply that by the log, that's give you a factor. That's the explanation of numbers here.

The next slide here shows you the kind of where the issues are according to this metric.

Now, these are the TLDs. The interesting thing here is that there's only one kind of legacy TLD shows up on this list, and [inaudible] everything else here is a new gTLD. And these numbers kind of reflect what you'll see. And I put a few different sources here, and you'll see there's an overlap amongst the sources as to where the problems are. So, you can see there's an issue then the new gTLDs are definitely having problems with abuse on the TLDs. And you can see by sheer size. You can take a look. It's about [inaudible] dot top. And you can see there's over half a million domains seen and over 300,000 that have been classified by Spamhaus at least as being bad. And there's some interesting that start showing up when you start taking a look at this. Dot gdm is – GDM stands for generic domain name by the way, which we found out because of – we were like why are all these .gdm domains showing up as malware CMCs on exploit sites. [Inaudible] internally. And this is when Spamhaus is seeing the same thing. And that's what GDM stands for. This exposes [inaudible]. This is a pretty decent metric to take a look at where things are going on.

These are the registrars that are having. And based on the same kind of formula where things are – Spamhaus at least is observing problems. Most of these are in – they're in APAC region, China, Japan – I believe GMOs to be [inaudible] in Korea. There's a couple like Moniker. It's more of a larger scale one. And you though the numbers here, I'll just compare that to the index number here versus the index number on the TLDs. There is a rapidly diminishing tail here.

So, on this one is only like the top six or so. And on this one it's really the top four or five that have more pronounced problems. Out names is a real problem right now. That is one that we are seeing massive amounts of abuse with them. And that's across the board. Anecdotally there's a lot of discussion around that particular registrar and their operations. So, that's one. If you're [inaudible] number one problem child out there that's within the ICANN world of purview I guess out names of that.

Now, I see one of the questions, what are they doing? What is ICANN Doing about it? I know the Compliance department is working on the problem. I'm not sure what that entails. But that's the current one. We've had others in the past, and these things kind of go – oh by the way, the Number 2 and Number 3 on the list are owned by the same company. So, [inaudible]. I'm not even trying to do that. Domainer's choice. Those are small, but they're actually owned by the same company.

[Inaudible] that is another. It's similar to Spamhaus, but they have different methodologies, different people. Then they have a list they publish on their website. I've got those down on the lower right. It's kind of [inaudible] smaller. Their list just does raw. And this is where you see all the – they break it down by TLD. And so as you might expect .com is by far the most abused TLD out there. But that's half a million domains on 100 plus million. So, there's a percentage of their overall volume of domains. It's very tiny.

Obviously what shows up next is .com, which is a favorite of Spamhaus as well. So, we're seeing even though these are as you might expect

legacy TLDs showing up because they are by far larger than most of the other spaces we're seeing large amounts of use on some of the same TLDs. One ccTLD. Oh no, actually there's two ccTLDs. I'm sorry. You also saw that too. Dot us is on there too. Dot us is another super marginal. Dot ru has traditionally has a lot of different kinds of abuse on it. Actually, driven marginally by malware, which [unintelligible] does a little bit more picking up than Spamhaus does, but that [inaudible] don't necessarily reflect.

The timeline on the [unintelligible] data is what's currently in their listings. I took a snapshot of this a couple of days ago. So, that gives you an idea of what it… So, basically they will age things. They will take things out once they disappear off the Internet or one there's a the TTL I believe is like 30 or 60 days. So, if they seem batched up within that time period, they'll list it and otherwise if they don't have another report of something bad they'll take it off.

You are welcome, Carlton.

Okay. So, a couple of anecdotes out of the [inaudible] folks that I was talking to them about this presentation. They gave me some feedback from dot [inaudible], and I already talked about that. One of the things is a TLD programs matter. So, a great example of this is .xyz versus .info at the singing registrar. So line one has a promotion going on. You can get .info or a .xyz for free. And the .info runs a pretty aggressive anti-abuse program. And it's really on top of things that are [inaudible] TLD and they take active action against it.

But XYZ, they have a program. I just don't think it's effective. And we're certainly seeing a lot of abuse within that TLD. And price is also… I already mentioned this before, but just a great anecdote on this was a promotion on .work. It was going for 50 cents on GoDaddy and they were seeing a lot of, you know, stolen registrar registrations. And the price went up to basically $4.00 and that abuse about disappeared overnight. And there was no other – GoDaddy didn't change any of their other operations. They just raised the price. And the abuse went down. So, it's a pretty good indicator that criminals are set to the price incentive.

There's a couple of big promotions that have been [inaudible]. I'm sure some of you saw that, "Hey, get your whatever for a penny." And there were a couple of TLDs that did that. As you might imagine, I saw a lot of bad registrations amongst all the other stuff. So, they do care. And despite the fact that it would be setting up dodgy adult content sites would be something you want to do without xxx or .porn, we very rarely see any abuse on that. But those TLDs are very expensive. They're $40 to $60 per domain per year. So, it's pretty good indications out there that price does matter a lot. Okay. Excuse. All right.

The final set of numbers that I want to go through is the unpublished unfortunately APWG goal phishing survey. And this is actually expired. I think too late to ask him to present today, presented some of this data to SSAC in Helsinki. Latest data from APWGs, our whole look of data 2015 plus, the Anti-Phishing Association of China. I'm not sure when we're going to publish this, because Greg and I haven't been able to get together and do the fancy graphs and tables. We've got all the data. We just have to do the publishing of the paper and both of us have been

really busy. But anyways, the idea is we're looking at phishing. And this is only fishing it's not all the other abuse. It's a good indicator of where things are going on.

Top line numbers here if we've got over the year, and these are unique verified attacks. The actual report is actually we hired [inaudible]. But these are ones where we actually verify and monitor. And those [inaudible] I would actually give you the – I've got some table to show you how that is versus history. That gives you an idea there's no, you know, these are how many were used for fitness. So, like the TLDs used for phishing are 355. A hundred and thirty-five of those actually had a registration which means the other 120 or 220 merely had compromised domains with them. So, again, this is the criminals breaking in and stealing the resources versus the criminal creating the resources through some methodology. So, and those have different techniques we're dealing with them.

And then so some of the things we saw was a lot of domain shadowing. Mentioned that already. That's the breaking in and adding new records. Traditionally we've had about 20% of the domains involved in phishing were registered by bad guys at least since about 2009, 2010. It spiked up again. So, the new gTLDs were problems. I'll show you the data on that. The price we definitely saw the cheaper ones followed. The use of URL shorteners has increased again. That's things like Bitly and Google if you ever use those.

And if you take a look at the operators behind some of those TLDs you'll see it's the same operators behind is kind of the one that is the owner is the TLD is those problematic TLDS go back to in some cases the same

owner. So, it's kind of looking at it like it's a policy or implementation issue with them.

So, here's what the statistics look like kind of a year-by-year. Sorry. It's right to left on this one. So, the latest here is on the left. And you can see it's basically been, it jumped up in 2014. And it's actually declined slightly in 2015. I know it's gone back up in 2016. So, but despite the fact that the amount of the tax and domains ease went down the number of malicious registered ones went up. And of all the hundreds of thousands of domains that we saw only 275 were on [IDM's] [inaudible] domain names. Okay.

And then, let's take a look at the scores that were in there. So, we do a scoring methodology similar to Spamhaus's but what we do is we take the… well, in this case we take the number of domains we've seen fishing and we divide it by the number of actual domains in the registries. That account includes all the parked ones, all the ones that aren't even on the Internet but are registered. We have those numbers, at least for most of it asked. DOM is domains over management. That's what that stands for. It's not the [inaudible] TLD that's DOM, the domains of the management. And some of these are estimates because they don't share that data. But most registries share that data with us or publish it themselves.

And you can see that the highest attacks… These are attacks. These don't necessarily mean that there's a malicious registration or what have you. Well, these are individual attacks, and you can see that [.ly] is like a big outlier here. What is up with that? Well the reason for that is Bitly. This is where having a… So, if you're a registry operator, you've

got to be aware of who's running services on your TLD to maintain your reputation. Bitly ends up being the [forwarder] to a lot of malicious stuff, so it's the thing that gets reported. That drives up the score here tremendously, because a whole bunch of bad URLs reported on Bitly are individual attacks because of the nature of Bitly. That drives that kind of stuff.

That's an interesting thing that we'd pull out of that. The way, your methodology for scoring things really matters, so you really have to understand the data and what's going on.

Let's take a look at – this is [not a] unique number of phish. I'm sorry, unique number of domain names used for phishing, which is different than the number of attacks, because an attack can be – you have several attacks on the same domain name. That was the first slide.

This slide looks at just individual domain names used, whether how many [inaudible] one or 100 attacks on it, it doesn't matter, we're going to count it once. So that actually you see Bitly drops completely off, because almost everything in .ly was under bit.ly, so its actual [inaudible] here is almost zero, it is close to zero.

But you see here that Venezuela, and many or most of these are ccTLDs. If you know the kind of background of these, some of these, like Thailand, has always been a problem child, and the reasons for Thailand having problems is that a lot of their universities and government sites are not run by – they're run by very junior systems engineers, and they're always getting hacked.

So almost everything in Thailand that's been in an attack was a hacked domain, whereas you have things like .cf, .gq, .ml, which are being run as kind of the marketing style of ccTLDs, where they're promoting them for something other than the country code use, and a lot of them are being run by Freenom, and they're basically giving away domains. As you might imagine, because bad guys like free or cheap, they're gravitating towards those.

Because we do this division, there are very large numbers. For example, .cl. I'm trying to remember, .cl was, I think I don't remember them being in that [inaudible]. I'll have to take a look at that. That doesn't seem right to me, make sure I copied and pasted the numbers in there properly. But I know Chile was on the list. A couple of Americas in here, but mostly – well, Venezuela and Chile would be South America at least, or central, to answer that question.

The last one here, this one gets to the malicious registrations. These are the ones that are actually registered by the bad guy. Here's where you'll see that Venezuela's problem is actually in the registrations of domains. This is more of a control problem of how they're allowing registrations to occur. And so the ones that are showing up here, this is where you see .cf, .gq, .ga, .ml, .cc, .pw. These are all being run as those kind of marketing style domains.

And then you see some of the new gTLDs pop into the list here. You have .science again, we saw that already. .top, .party – I guess they're having a party on this stuff. And then .com actually… This is actually interesting. Dot com is about 2.7 [inaudible] 10,000. We're going to use that as kind of a statistical average or benchmark, as .com is so broad,

it's hard for that number to move much. So anything below that – we have a couple below that – probably aren't too bad, relatively speaking. So what that tells us is that the problems with registrations are really concentrated on everything kind of above this line, at least when it comes to phishing. That doesn't cover a lot of other stuff, that's phishing.

Alright. This stuff here is – things are covered for the most part. It emphasizes that cost matters, and that these programs do make a difference, but we find they don't always. Like in the case of .biz, they have a pretty good anti-abuse program, but they were still seeing a fair amount of it.

We continue our highlights around registrars in Asia, and that's across the board. We're talking to many different security companies and people dealing with these issues. The anti-spam companies, that's where [if we're] having a problem, registrars are typically in that group, in that geography.

Then some of the resellers are definitely – we hear plenty of anecdotes about it and we see it as we're doing operations where the reseller will pop up, purchase a bunch of stuff, they get a bunch of complaints, they'll ban that reseller and they'll pop up with a new name, maybe with that same registrar or with a new registrar. So they're doing that fairly regularly.

I would say most of the new gTLDs are doing pretty well. We don't see too much abuse at the new gTLDs. Where we do see it though, they're

having big problems, so it's very concentrated, I would say, based on the numbers.

Okay, to wrap up here, I have a couple of other [inaudible], some practical things to take away here: if you own a domain name, make sure you get that locked down so you don't get these hijacking or domain shadowing folks coming in.

Don't use the same password for your domain registration that you use for other things. All that kind of common sense stuff. If you want to avoid this kind of spear phishing and business e-mail compromise, turn on e-mail authentication. There are things called SPF and DKIM that are standards, and this other reporting one called DMARC. These are all typically available from either your registrar or your hosting provider who's hosting the domain name.

And if you have a business, DNSSEC is a good thing, because, again, some of the spoofing stuff, it helps you take care of that. So it's a practical use for DNSSEC. And get that security that you think you should have.

If you're running a business, one of the things you need to be aware of is looking for things like that data exfiltration, which is something that most products don't do. There are some out there that do that, but it's something to be aware of, especially since it's becoming more and more prevalent in mass market malware, versus kind of the state actor stuff that it used to be.

And user education programs are really effective in terms of spear phishing. I was very skeptical about them in the past, but I've seen the

results, and I'm a believer at this point. Basically, give your users tests. As an individual, make you're taking advantage of the browser filters and things like that that Chrome and Microsoft provide.

If you want, you can use an open DNS service for clean DNS services. In other words, they try and make sure you're not going to malware and things like that. Google DNS is great, but they don't do anything to actually change anything in the DNS. So if you're worried about that kind of stuff, you probably want to use somebody who's doing that kind of thing, and some of your ISPs will do that for you as well, so you should check with them and see what they provide.

Make sure you're using NSPM software, and your own – I forgot to put it in here – antivirus software.

Then there's the Stop, Think, Connect campaign, which is beginning in more and more countries, which is just the common sense of, "Hey, if there's a message that's really urgent that's unexpected or there's an offer too good to be true, think about it before you click on it." These days, if you click on it, then you might have that hit that exploit site.

Yes, Carlton, the Jamaican [inaudible] APWG has been pushing their Stop, Think, Connect in a worldwide thing. Many different countries have adopted – I think organizational [American states] has also been doing that.

Yes, Ricardo, I saw your question there. Yes, feel free to use those numbers. These numbers, while they're unpublished, they're the final data that we have, so I'm perfectly willing to let people use the data

here, since I'm not sure when we're going to publish this. If you can do use it, feel free to do so, and if you have access to the presentation.

The final slide I have here is some policy questions to consider based on what's going on here. These are things to think about, I'm not trying to espouse one viewpoint or another, but in general, are we doing a good job of tracking, measuring and reporting abuse consistently?

As you saw, just from the way I was looking at different numbers, your metrics matter. How you decide to track things, how to score things, those matter, and everybody does it a little bit differently, and those end up driving decisions. More importantly, are we even gathering statistics and making [them] transparently recording those?

In order to find a lot of these statistics, you have to go to a place like Spamhaus or to the APWG or things like that. There hasn't been a lot of recording on these kind of things done by a kind of – what I call quasi-regulatory authority, or what have you. ICANN certainly doesn't do that, for example. The Compliance department will give you all kinds of information about reported complaints, but they don't have kind of, "Here's where the abuse is."

What are we doing with protection mechanisms? Domain shadowing is becoming a real problem. Many years ago, SSAC published two references, [One is] SSAC 40 and SSAC 44, about protecting registrants and registrars from these kinds of abuse. Obviously, given the problems we're seeing, those have not been fully implemented by all registrars, and frankly, the registrars that are being used for domain shadowing are some of the big ones that have – the bad guys like the fact they have

APIs they can use to control all those domains they get access to. So there are some issues there, potentially.

We have these large-scale abuse issues, do we have adequate policy to kind of have a graduated response to that so that this stuff doesn't go on for years and years, which we've certainly seen happen in the past? What are the ways we can have people in the industry learn from each other about the attacks that they're seeing?

For example, if I determine that I have this methodology that people are using for breaking into my user accounts or domain shadowing, once I figure that out, I implement that, then they go on to the next registrar. Are we doing a good job of sharing that kind of information so that all registrars are registries can protect themselves?

And there are the ways we can provide better, more consistent ways of recording these kinds of abuse. There's actually a coalition and others are working on this, and that's why I threw this in here, but it's clear for from kind of the data and from the feedback from people dealing with issues that there's a wide variety of ways people classify things, they report things to service providers, and service providers react to those reports. Would it be good for folks to take a look at either – can we do something to foster that, a better way of dealing with these things? Because they do affect the entire community.

So that was it for my presentation, and I thank you for your time and dealing with all those communications issues. I talked a little long. I'll turn that back over to the moderator.

TIJANI BEN JEMAA: Thank you very much, Rod, for this wonderful presentation. Unfortunately, we are only six minutes before the end of this webinar, so please, if there is any question for Rod, please raise your hand. I don't see any, so I will ask perhaps Terri to [pop quiz] –

OLIVIER CRÉPIN-LEBLOND: I have my hand up.

TIJANI BEN JEMAA: I didn't see it. So go ahead, please.

OLIVIER CRÉPIN-LEBLOND: Thanks very much, Tijani, and I definitely had my hand up, I don't know why it doesn't show on your screen. Thanks very much for this, Rod, very interesting indeed. I was just going to ask one thing: Architelos used to do these reports as well, and as you know, they folded. Have you taken over the data that they also have? Or I think you were involved with the work that they were doing as well in this anti-phishing stuff.

ROD RASMUSSEN: Greg Aaron was the one who actually was my partner in doing the APWG work who was the one who was involved with Architelos. My company provided some data to Architelos, so we were a component of what they were reporting, but they were pulling things in from multiple sources.

So nobody has really taken up that reporting capability that they were doing, that they were providing as a service to the community, There's some desire to have that done within APWG, and it just hasn't come to fruition. It's an all-volunteer organization, and the volunteers have been volunteering for ten years, so it's been a bit tough to get something new stood up. But hopefully, we'll have somebody come along and do a better job of getting this data out there. As it is right now, we had to dig into things that various security companies are tracking in order to put this presentation together.

TIJANI BEN JEMAA: Thank you very much. Olivier, you still have your hand up.

OLIVIER CRÉPIN-LEBLOND: Yes, thank you, Tijani. I have two more questions, if that's okay.

TIJANI BEN JEMAA: Yes, but very quickly, because we are – yes, go ahead.

OLIVIER CRÉPIN-LEBLOND: I'll be very fast. The first one is to do with the data that you presented to us in this current presentation. Are we able to make use of this? Because all the way until the more recent ICANN meetings, I've had people in the contracted parties, and indeed the people on the Board coming to me and telling me there's absolutely no proof whatsoever that there's any kind of malware being worse on the new gTLDs than in the legacy TLDs. And clearly, we're seeing in this presentation that

you're giving us – unless I'm completely wrong and I'm hallucinating – is that there certainly is a problem with those new gTLDs.

And secondly, I have noticed in the chat that there was a question from Ricardo Holmquist from ISOC Venezuela, and understandably, with .ve being very highly qualified on the list of the malware and so on, he was asking whether he could use these numbers to be shown to the local ccTLD, as ISOC Venezuela might have some leverage with them because obviously, there is a serious issue with it.

ROD RASMUSSEN: Yes to both of your questions, and actually, I did answer – you may have missed that, I did respond to his chat question, but yes, and that's on phishing, just to be clear, the Venezuela numbers, but yes, please, go ahead and use that with the folks in Venezuela. The APWG unpublished numbers, I'm giving everybody who's got access to this permission to go ahead and use those, because those are our final numbers and I'm the author, so go ahead and use them.

And then on the other, the Spamhaus and [inaudible] those are published on our website. So those are already public, so all that data is good to go to use.

TIJANI BEN JEMAA: Thank you very much. If there are no more questions, I will ask Terri to go ahead for the pop quiz. Terri?

TERRI AGNEW: Thank you very much, Tiajni, and we do have two pop quiz questions. Let's see if everyone was paying attention.

Pop quiz question one: what is domain shadowing? Please cast your votes now. And once again, the pop quiz should appear on the right hand side of your screen.

And, Rod, I'll go ahead and broadcast the results. If you could please share the correct answer.

ROD RASMUSSEN: The correct answer is B, but I do like the fact that somebody picked, "Discreetly following a domain name down the street in a '72 Chevy." That's good. B is, "Compromising good domain and adding [inaudible]."

TERRI AGNEW: Thank you, and pop quiz question two: data shows that domain name abuse tends to correlate to low prices for domain names with some exceptions. True, or false? Please cast your votes now.

Rod, I'll go ahead and broadcast the results. If you could please share the correct answer.

ROD RASMUSSEN: The correct answer is true, and at least from the data that we have for this presentation today and the data we've seen, but for the one person who still wasn't satisfied, okay, we'll go get some more data for you.

TERRI AGNEW: Thank you. Tijani, would you like me to go into the evaluation, or would you have any closing comments before we went into the evaluation?

TIJANI BEN JEMAA: Go ahead, please.

TERRI AGNEW: Thank you. We'll go ahead and move into our evaluation of today's webinar. Once again, if you could please stick around just for a few moments to collect some data, but we thank everyone for your time today.

Evaluation question one: how was the timing of the webinar for you? Please select your choice now.

Evaluation question two: what region do you live in at the moment? Please select your choice now.

Question three: how many years of experience do you have in the ICANN community? Please select your choice now.

Question four: how is the technology used for the webinar? Example, the audio, the phone bridge.

Question five: did the speaker demonstrate mastery of the topic?

Two more questions to go, we do appreciate your time. Are you satisfied with the webinar?

And one final question, and I'll leave this up on screen. Please take your time to complete it. What topics would you like to cover for future webinars? This is an open question, so type in your answers now.

Once again, we thank everyone for joining today's webinar, and please remember to disconnect all remaining lines and have a wonderful rest of your day.

CHERYL LANGDON-ORR: Thanks, Terri.

JULIE HAMMER: Thank you, Terri. Just before we all sign off, can I just acknowledge the effort that Rod put into preparing and presenting this webinar, and on your behalf, extend our sincere thanks to him? Greatly appreciated. Thank you, Rod.

ROD RASMUSSEN: My pleasure.

TIJANI BEN JEMAA: Thank you very much, Julie, and thank you, Rod. Thank you, Julie. Thank you all our interpreters, our staff. Thank you all. Bye.

TERRI AGNEW: Thank you, everyone. Once again, the meeting has been adjourned. Thank you very much for joining. Please remember to disconnect all remaining lines, and have a wonderful rest of your day.

JULIE HAMMER: Bye, everyone.

[END OF TRANSCRIPT]