SAN JUAN – GAC: Encontro do PSWG
Terça-feira, 13 de março de 2018 – 8h30 às 9h30 AST
ICANN61 | San Juan, Porto Rico

CATRIN BAUER BULST: Bom dia para todos. Muito obrigado por estar aqui nesta sala e não estar lá fora no Caribe com o sol e o lindo clima. Obrigado por dedicarem este tempo. A reunião do Grupo de Trabalho de Segurança Pública. Esta é, então, a reunião oficial deste grupo dentro do GAC. Meu nome é Cathrin Bauer Burst. Aqui está a Laureen Kapin. Uma das duas vice-presidentes. Temos dois assuntos importantes para trabalhar na ordem do dia, na agenda de hoje. Vamos falar, então, sobre o plano de trabalho do PSWG e depois, vamos falar também do trabalho que estamos fazendo com do Diretor Técnico e o que é a ferramenta do DAAR. E vamos dar a possibilidade aos outros co-presentes para que possam falar.

LAUREEN KALIN: Eu estou na Comissão Federal dos Estados Unidos de Comércio. Estamos concentrando, no que é proteção ao consumidor e agradecemos a presença nesta primeira sessão do dia, que vai das 8:30h às 9:30h. Também vão escutar dizer: "Não, mas depois das 9:30, vocês vão continuar?". Sim, sim, é verdade. Porque

vamos mudar de assunto, vamos nos concentrar depois no que tem a ver com o sistema do "who is" e o GDPR. Mas vamos ter uma dose muito grande deste grupo de trabalho. Durante hoje de manhã. Então, eu espero que todos fiquem para a próxima sessão e que seja interessante.

IRANGA KAHANGAMA: Eu sou Iranga Kahangama e sou, também a... Washington DC com o FBI. E eu vou trabalhar também, vou falar alguns dos temas que tem a ver com o abuso do DNS e que tem a ver, também, com o DAAR. Vamos ver algumas apresentações e também, algumas formas nas quais nós podemos apoiar as políticas e recomendações, ou fazer alguma contribuição ativa da atividade do DAAR. Porque nós pensamos que vai ser de benefício para toda a comunidade da internet. Então, vamos continuar falando um pouco, também, depois sobre esses assuntos.

CATRIN BAUER BULST: Muito obrigada. Laureen acaba de fazer uma boa sugestão. Aquele que seja membro do Grupo de Trabalho de Segurança Pública, eu peço que levantem a mão. Porque há muitas pessoas na sala que tem interesse em nosso trabalho e talvez, também, a medida que continue o dia e a semana, podem estar interessados em falar conosco. Então, peço, por favor, que

levantem a mão, os membros do grupo, para que todos os reconheçam e saibam onde é que estão.

LAUREEN KAPIN: Essas são as pessoas e tendo algumas dúvidas, não só nós que estamos aqui na frente, mas outros membros. E todos eles estão dispostos a falar e a responder as suas perguntas.

CATRIN BAUER BULST: Da reunião do domingo, sabem que nós vamos adotar o plano de trabalho para o próximo período deste grupo de trabalho. Falamos disso, a um nível mais alto no domingo passado. Mas hoje, vamos aprofundar um pouco. Se é que alguém tem algum outro comentário antes de adotar alguma parte no comunicado do GAC e que possam contribuir para o plano de trabalho. O primeiro objetivo estratégico tem a ver com a mitigação do abuso do DNS. Iranga, tem aqui um comentário a respeito dos diferentes pontos.

IRANGA KAHANGAMA: Obrigado, Catrhin. Como mencionei antes, esse é um dos principais planos de trabalho. O objetivo é que a ICANN esteja numa melhor posição para tratar este uso indevido do DNS. Eu sei que há muitos relatórios. O CCT também emitiu o seu. Eu acho que é um dos grandes programas, que temos na

atualidade. Eu peço que, por favor, olhem a tela aqui à direita. Como eu já falei, há vários projetos e informação sobre as atividades vinculadas com estes assuntos. Há, também, o índice de insalubridade da praça de GDID, o que tem a ver com a iniciativa de dados abertos da ICANN. isso também tem a ver com colocar alguns números a este abuso. A esta insalubridade, a nível macro. Então, estamos numa melhor posição para informar sobre esses usos indevidos. Vou passar um pouco por cima da outra informação aqui. Também, estamos já, no princípio. Nossa ideia é ter uma linha de base para entender alguns mecanismos genéricos, que aceitam todas as partes da comunidade, que todos entremos em acordo ao respeito deles. E o que faz o trabalho é o novo trabalho. Um dos assuntos com os que tivemos falando é o SSAC. Eles tem várias iniciativas, também, que são interessantes. E nós gostaríamos de participar formalmente do trabalho, que eles estão fazendo. Eu acho que nesta reunião, há uma sessão às 15:15h, amanhã. É uma reunião aberta e todos disseram que podiam participar. Então, vai ser interessante ver nessa reunião, alguns dos aspectos de segurança nos quais eles estão trabalhando. O serviço de registração e os aspectos técnicos vinculados com isso. Eu acho que tinha que ser muito importante, principalmente, porque há considerações vinculadas com o GDPR. Há pessoas que estão muito orientadas à segurança. Então, a ideia seria estabelecer uma relação um pouco mais formal com eles para ter um canal

de diálogo. É basicamente isso, que estamos tratando de conseguir. Claro que podemos receber todas as suas ideias. Há vários temas, que são atuais e que tem a ver com o abuso do DNS. Temos pouco largo de banda agora, mas eu acho que estamos funcionando bastante bem com o trabalho que estamos fazendo. Consideramos este tema de alta prioridade.

CATHRIN BAUER BULST: Antes da Laureen, que vai passar o terceiro ponto das medidas de proteção ao consumidor. Eu quero lembrar os membros do GAAC, que os senhores tem uma cópia desse grupo de trabalho, como anexo dos documentos enviados. E também, como o anexo ao ponto 11, que debatemos no dia de domingo, na agenda. Então, podem consultar aí, o plano, naquele anexo.

LAUREEN KAPIN: Muito bem. Falando um pouco do que são as medidas de proteção do consumidor. Este foi um tema, que tem a ver com a equipe de revisão da confiança deve ser competência do CE. Consumidores se concentram nessa medida de proteção. Agora, esse tema é uma continuação do trabalho, que já começamos, e que lutar por políticas, que protejam o público online. Este seria o objetivo geral ou o mais importante desta parte do plano de trabalho. Nós participamos em diferentes revisões, pertinentes, também. E também começamos uma coordenação com

diferentes partes da área da organização da ICANN, que tem a ver com segurança e cumprimento contratual. Aí com a comunidade, também, para falar desses assuntos. Porque todos tem um interesse em manter um entorno que seja seguro para os consumidores e também, que os consumidores confiem para continuar utilizando a internet. Há diferentes partes interessadas, diferentes áreas de trabalho, que incluem o que são os procedimentos posteriores. A introdução dos números de ccTLDs, também o que é um PDP, também o que é a habilitação de serviços de privacidade e reapresentação, diferentes áreas de trabalho, que vão continuar.

CATHRIN BAUER BULST: Eu vou falar dos seguintes pontos, que são sobre prestação de contas e que estão na próxima folha. E que tem a ver com a exploração e abuso do DNS. Quando falamos de prestação de contas é de responsabilidade, o que estamos buscando é alguém que assuma esse ponto, que trabalhe com esse ponto. Há diferentes áreas de trabalho, que tem a ver com a segurança pública e são pertinentes ao trabalho do GAAC. Também é um trabalho sobre segurança pública e o que queremos melhorar na capacidade que temos. Porque somos muito poucos, os que compartilhamos a carga desse trabalho. Então, se alguém de vocês, um de vocês querem participar numa coisa importante e interessante. Eu peço que se aproximem, depois desta reunião.

LAUREEN KAPIN: Sim, claro! Aqui é um de nós, pedimos à vocês, que nos ajudem a os ajudar..

CATHRIN BAUER BULST: A respeito da responsabilidade por prestação de contas. Vamos falar um pouco mais na segunda, meia hora desta reunião. Porque, como dizia Iranga, antes, estamos tentando identificar fontes de dados que possam nos ajudar para avaliar a política existente de forma mais confiável. E também, fazer as seleções adequadas para as novas políticas, como podem ser qualquer rodada posterior, que exista para os novos ccTLDs. Então, temos que ter as fontes de dados corretas, os dados corretos e disponíveis para esta nova posição, quando sejam necessários. Também falamos de como evitar a exploração do DNS para perpetrar um abuso. Aqui, vamos tentar nos concentrar em identificar diferentes tipos de abusos indevidos. e também, nós vamos se beneficiar do trabalho do SSAC. E também, do lado da política, ver como podemos ser mais eficazes e evitar parte dessas coisas. Também é uma área de trabalho, que tem a ver com a luta do abuso contra as crianças. Especialmente, queremos ver o que acontece com a eficácia das medidas de proteção propostas pelo GAC na sua época para proteger especialmente as crianças nos lugares, que tem associações

como confiança, que podem ter a ver com o ponto "kids". Há uma expectativa legítima de parte dos usuários, de que esses sejam um espaço seguro para as crianças. Então, as medidas de proteção do comunicado de Pequim... de Beijing, tem que ser garantia de eficácia. Também, podemos pensar em adotá-las para as próximas rodadas dos novos gTLDs. Há uma área de trabalho e nós vamos falar muito mais aqui. Mas esse seria um pouco a área, da qual eu quero falar e eu sei, que a equipe italiana do GAC se concentrou muito nesses temas. Antes de fechar esta parte, eu quero ver se alguém tem algum comentário, ideia para compartilhar. Vamos continuar, então, com o objetivo estratégico, que se concentra no RDS, em especial. Tem a ver com o "who is" e com acesso aos dados de registração.

LAUREEN KAPIN: Bom, isto, como eu já falei, eu vou dividir. Porque vamos falar deste tema com mais detalhes, como eu disse antes, depois do recesso para o café. Isto é apenas para mencionar e que saibam, que o sistema do "who is" e todos os benefícios e a responsabilidade associadas, fazem parte da nossa área de trabalho. E nós nos concentramos nesta parte na última etapa do trabalho.

CATHRIN BAUER BULST: Isso leva ao PDP RDS seguinte geração. Falou, Alis Munha, outro dia não sei se hoje quer falar alguma a respeito. Não? Muito bem. É uma coisa que continua em andamento. Também está a exatidão dos dados de registração. Os senhores sabem que há tempos está se falando disso. Agora, há alguma implementação, como para verificar o que é sintaxe na exatidão da registração dos dados. O que a comunidade não falou ainda é sobre a verificação de identidade do registratário. E continuam do ponto de vista da segurança pública. A verdade é que as opções que há para melhorar a qualidade, o que tem a ver com o GDPR no mundo do ccTLD. Eu acho que ainda há possibilidade de que isso seja mais confiável sem maiores custos. Veremos, então, como vão esses esforços ou como podem traduzir no mundo dos gTLDs.

IRANGA KAHANGAMA: Eu quero adicionar uma coisa. É muito importante, dentro do plano, esta sessão. Porque temos que pensar que o GDPR também pede uma exatidão nos dados. E isso, então, faz parte da nossa responsabilidade. E precisamos dos dados. Não nos concentramos aí, porque ainda estamos tentando manter os dados e o acesso. Mas temos esse segundo passo ou etapa, que realmente, de que esses dados sejam exatos. Que temos que levar isso em conta, porque vai ser uma ferramenta muito importante e uma coisa, que vamos ter que incorporar este

tema na seguinte versão do "who is". Porque são os requisitos do GDPR, sermos um pouco mais exatos.

CATHRIN BAUER BULST: Obrigada, Iranga. Último ponto, neste segundo objetivo estratégico, é a verificação da implementação. Ou seja, como é o cumprimento da missão da ICANN com relação aos RDSs. O importante é que temos uma equipe de revisão. Então, foi indicado, designado através do GAC, a representante dos Estados Unidos e da Interpol. E eu, como, para participarmos. Então, temos que ver o que vai acontecer, quando nos reunirmos na seguinte reunião no Panamá. Laureen, por favor.

LAUREEN KAPIN: Bom, este é objetivo estratégico 2. Alguém tem algum comentário sobre todos esses pontos, incluídos nesse objetivo estratégico? Muito bem, então, vamos continuar. E passar hoje, à princípio, ao objetivo estratégico número 3. Aqui, vemos os fundamentos, que tem a ver com gerar uma operação flexível e eficaz do PSWG. Isso tem a ver com o nosso marco de organização e os nossos procedimentos. Então, vou ver que aqui falamos de desenvolver um plano de trabalho, que é o primeiro passo. Depois, fortalecer a liderança como mencionamos domingo. Nós queremos ter uma grande reserva, porque há muitos temas importantes e queremos, que as pessoas se

concentrem nesses diferentes pontos. Também, queremos fortalecer a quantidade de membros. E temos... uma das ideias é que se vamos falando com as autoridades do GAC e é importante, que todos os membros do GAC considerem nomear e difundir e chegar as autoridades de aplicação, especialistas em segurança pública dentro de cada governo. Porque essas pessoas existem em cada um dos países. Pessoas que conhecem muito sobre o que é a investigação na linha de fogo, na frente. Sabe como saberem detectar atividades em rede, que eliminam acesso, especialmente, os que tem a ver com DNS. Sabemos que, às vezes, isso é uma coisa muito técnica e complexa. Mas vocês tem especialistas no país, com os quais podem consultar. Então, nós incentivamos aqui, trabalhem com eles de forma, de maneira formal. Que entrem em contato com eles, que indiquem como assessores de grupos de trabalho em Segurança Pública. E que possam participar nas videoconferências, na lista de distribuição de correios eletrônicos. Se é que existem os recursos, também podem participar nas reuniões. Então, é importante que todos participem de forma ativa em todos esses temas que tem a ver com segurança pública. Queria destacar esse ponto. E também, somos um comitê assessor e somos um grupo de trabalho do comitê assessor governamental. Então, temos que ter a certeza, de que estamos nos comunicando de maneira uniforme e coerente com o GAC e com suas autoridades, para que saibam em que estamos trabalhando.

Nós vamos falar se há algum tema importante , que exija ação rápida de vocês. E tivemos um exemplo, há pouco tempo, porque pedimos que analisassem coisas que eram complexas, que trabalhassem com rapidez. Não é a situação ideal. Mas, infelizmente, é a situação, na qual estamos ou estávamos e queríamos ter a certeza, de que estávamos fazendo tudo como a melhor eficácia possível. Informar do que está acontecendo, dar também um alerta para que revisem algum ponto que tem a ver com o PSWG e receber a contribuição, as opiniões para trabalhar de maneira conjunta. E que o conjunto, o produto final reflita uma posição de consenso dentro do GAC. esse é o nosso plano e eu respeito. Também, sempre temos presente, que queremos escutar, o que os senhores tem que falar sobre o que fazemos bem e o que podemos melhorar. Eu peço que não tenham vergonha, não sejam tímidos. Porque queremos falar com vocês nos corredores, por telefone, cada vez que os senhores acham que devemos fazer algum ajuste, estamos aqui para escutá-los. Este é o objetivo estratégico 3 do plano de trabalho. E eu quero receber comentários, perguntas a respeito disso, por favor.

JASON: Eu sou Jason do PSWG, representação do Canadá. Em Abu-Dhabi, se mencionou que esse grupo era homogêneo no sentido de que existiam muitas pessoas da América do Norte e Europa

Ocidental. Mas quero dizer, que gostaríamos de diversificar a composição do nosso grupo. E se vocês tem pessoas, que consideram que seriam bons candidatos para trabalhar com este grupo de trabalho de segurança pública. Por favor, se aproximem. Nós podemos falar como participar. Quanto mais diversos sejamos, mais fortes seremos. Então, eu acho que essa é a mensagem, que queremos transmitir. E o fato de que há muitos da América do Norte e da Europa Ocidental, não significa que não queremos receber as opiniões de outras partes do mundo. Realmente, gostaríamos de contar com elas. Por favor, se aproximem e nós podemos ajudar, que vocês colaborem, que talvez, algumas autoridades da segurança pública se aproximem de nós.

CATHRIN BAUER BULST: Obrigado, Jason, por salientar isso. É muito importante. Quanto mais diversos formos, mais vamos mostrar a composição do GAC em pleno. Isto é muito importante, porque somos um grupo de trabalho, que os ajuda, a que façam a sua tarefa. E poderíamos funcionar melhor se mostrássemos diferentes posições que existem no GAC. Nesse grupo de trabalho, grande parte do que fazemos não se faz nas reuniões. Fazemos ligações mensais em todo mundo, em todos os meses. Há ligações semanais, daqueles que estão com temas, todos os dias. Se voc6es querem indicar algum especialista, que já sabe que não

vai poder assistir as reuniões, isso não é fundamental. É claro que é melhor se podem estar nas reuniões presenciais de vez em quando, mas a maior parte do trabalho que fazemos é feito fora dessa reunião. Mas com a participação remota. Quero encorajar todos aqueles que se preocupam com os recursos. Para investir nesse trabalho. isso não vai prejudicá-los, porque não é necessário que estejam fisicamente presentes nas reuniões. Vou parar por aqui. Se vocês tiverem algum comentário sobre este ponto 3 ou se alguém estiver tão empolgado, que queira se somar ao nosso grupo. Se não houver mais comentários sobre esse tema, passaremos ao objetivo estratégico 4. O que a realidade tem a ver com fazer difusão externa e aproximar-nos a outras comunidades interessadas, fora desse âmbito. Estamos avaliando o que estamos fazendo no nosso plano de trabalho. E um dos pontos principais é estarmos certo de que ao estabelecer as nossas prioridades, elas sejam as certas. Mas para isso, temos que falar com aqueles de vocês, que estão aqui e com outros fora desta sala. Para ver o que que está lhes afetando, quanto as políticas, que estão se desenvolvendo aqui. Como, quais são as oportunidades para fazer melhoras, os grandes problemas que podem estar surgindo e querem que o nosso grupo trate. E dê a sua opinião ou informe ao GAC a esse respeito. Também, estamos trabalhando para desenvolver tomada de consciência do nosso grupo por parte dos órgãos governamentais. Para que todos os organismos, todos os países

estejam a par disso. Não se trata apenas da polícia. Outras questões vinculadas com a política pública e que se refletir, também estamos trabalhando para eliminar as barreiras para a participação. Não eliminar, mas diminuir. Ou seja, dar melhor informação. Talvez, estejam familiarizados com isso. Quando explicamos, o que é que acontece na ICANN para outra pessoa ou ficam dormidos ou depois dizem: "Bom, acabou já o tempo para a reunião". Então, é muito ... é um grande desafio ter as contribuições certas. Porque pensamos: "Bom, o que decidimos nessa reunião, o que que vai acontecer com esse tema?". Falamos, avançam as coisas. Mas isso leva muito tempo. Leva tempo chegar a uma conclusão por muitos motivos. Pode resultar... difícil que as pessoas estejam a par do que acontece aqui, entendem a importância do que aqui é discutido. E também, estejam em condições de identificar o por quê que eles importam e como podem contribuir a esse debate. Estamos trabalhando diferentes maneiras de reduzir essas barreiras ao acesso através de boletins, resumos breves, que dizem o que aconteceu aqui. Para que o nosso trabalho seja mais acessível para os que não estão tão a par das coisas, que a diário, acontecem na área da governança. Tivemos contribuições muito boas entre as reuniões da ICANN. Porque há muitos organismos, que não participam nesse trabalho e fizeram muitas boas perguntas sobre o por quê nos ocupávamos de determinadas coisas e compartilharam coisas, ideias que

tinham para que nós nos aproximássemos deles. Estamos trabalhando para por em prática essas ideias. E como podem ver, também, há espaço para mais voluntários, que se somem as nossas forças. Aqui pareceria que eu estivesse tentando arrecadar fundos, dinheiro.

LAUREEN KAPIN: Iranga vai falar sobre alguns esforços de difusão externa, que temos nessa reunião.

IRANGA KAHANGAMA: Talvez, esse seja o lugar para mencionar, que estamos começando a falar com o SSAC com mais profundidade, com mais intensidade. Para poder explicar-lhes, que é o que fazemos. Eles também tem um trabalho superinteressante. E no decorrer das nossas atividades, também falamos com registrador e registros, sobre as questões que tem a ver com RDS e "who is" para ver qual a visão de como estão desenvolvendo essas discussões. Essa é a difusão externa, que estamos fazendo. Vamos falar, também, sobre DAAR, DART. E há muita criatividade nesse âmbito. Então, se tiverem alguma ideia de comunidades que valem a pena... as que valem a pena tentar chegar, por favor, nos avise.

CATHRIN BAUER BULST: Obrigada, Iranga. Com relação a conhecer melhor outras partes da comunidade, quero lembrar-lhes de um evento que há com os registradores às :6:30h no terraço. Por favor, venham, se querem participar e conhecer outras partes da comunidade, melhor. Acho que com isso, concluímos. Não sei se há alguma outra ideia criativa ou alguém que quiser falar, que queira falar. Então, vamos finalizar com esse plano de trabalho que tivemos. Se tiverem alguma sugestão para fazer modificações nesse plano de trabalho, por favor, se aproximem de nós, enviem um e-mail para o final do dia de hoje. Então, senão pensaremos que isso já está finalizado e vamos enviar isto ao GAC para que saibam que se passou a aprovação desse plano de trabalho. Quer dizer, que agora, vamos para a segunda parte da nossa reunião, que tem a ver com a conversa sobre OCTO e DAAR. Vejo que o David está se aproximando. Obrigado, David, por ter um tempo e estar aqui com a gente. Sei que está muito resfriado. Lamento muito.

DAVID CONRAD: Bom dia. Peço desculpas pela voz. Estou resfriado, com tosse. Estou substituindo John, que parece que está passando muito bem, depois da gala. E o meu não é resultado da gala. Vamos passar para o próximo slide.

Estou certo de que a maior parte de vocês está familiarizado com o que é DAAR. Para aqueles que não sabem, DAAR é um sistema de informação, que estamos desenvolvendo com a ajuda do grupo cibernético, de ameaça cibernética, para de identificar o abuso, o uso indevido sobre todas as instâncias identificadas pelo GAC no comunicado da reunião de Beijing. O que tem a ver conforme, que é algo que vimos na ICANN. E também, o SPAM, que seria o correio, o e-mail não desejado. Como se diferencia a DAAR de outras ferramentas, que estão a disposição? Bem, é porque... pela quantidade de dados, que nós arrecadamos, basicamente, temos diferentes correntes de dados acumulados. E os dados são coletados e guardados para fazer estudos históricos. Vamos nos focar na multiplicidade de tipos de abusos, que podemos ver, onde se gera a informação, que é transparente e reproduzível para facilitar a comunicação para que se possam desenvolver políticas dentro da comunidade da ICANN. Eu já falei sobre isso. O que é importante salientar neste caso é que nós concedemos licenças a uma grande parte dos dados, que utilizamos para a DAAR. E talvez, possa não estar disponíveis, esses dados, em alguns casos. Para que, que se podem utilizar esse sistema? O principal objetivo é informar as atividades que apresentam ameaça em nível dos TLDs; para fazer estudos sobre os usos de domínio; também podem ajudar os operadores, registradores, registros, operadores de "back-end". Entender ou considerar como

podem gerenciar a sua reputação nos seus sistemas anti-abuso. Também, permite fazer um estudo das condutas de registros maliciosas. E também, se encaminha à assistir as comunidades de segurança operacional. Próximo slide.

Então, um dos conjuntos de dados, que utilizamos, são os dados de zonas TLDs. São coletados os dados das zonas de TLDs para a analítica de registros de gTLD. E usamos os serviços de dados de zona centralizado, onde é possível, também, fazermos transferência de zonas. O DAAR só vai usar os nomes de domínio, que aparecem na zona . Não vamos tentar procurar a base de dados do registro, só registradores, antes de que esses nomes estivessem incluídos em zonas. Atualmente, temos 1240 gTLDs, que nos leva a 195 milhões de domínios aproximadamente. Vários desses gTLDs se aproximaram para dizer que querem se participar da iniciativa DAAR. E temos que ver como que podemos incorporá-los ao sistema DAAR. O DAAR também utiliza o "who is". Só utilizamos uma parte pequena do "who is", principalmente, os dados dos registradores. Mas isso pode ser bastante problemático, pois DAAR se foca em tentar desenvolver um sistema que seja reproduzível para qualquer um. Então, nós geramos informação, que esteja disponível internamente dentro da ICANN. Nós estamos utilizando informação disponível para o público. Como resultado disso, tentamos extrair informação para milhões de domínios através

dos servidores existentes de "who is". E como muitos de vocês devem saber, isso pode ser realmente um desafio do ponto de vista da velocidade com a qual podemos nos movimentar. Se olharmos para o conjunto de dados de ameaças, utilizamos vários... tentamos identificar de maneira única, os dados, para que não haja muitos falsos positivos. Utilizamos os conjuntos de dados de abusos de URL ou de domínios múltiplos, para poder ver, principalmente, o que se associa com o phishing, malware, hopiness, spams. E também, tentamos gerar histografias e quadros gráficos com o foco colocado em dar ou mostrar como aquilo, que está fora da comunidade ICANN, veem, como eles veem o ecossistema dos nomes e domínios. Dentro de OCTO, nós não compomos as nossas próprias listas de blocos de reputação. Nós apresentamos um acumulado, imagem composta dos dados disponíveis através de entidades externas. Essas entidades essas listas, que bloqueiam as ameaças. DAAR é que colhe todos os dados de abuso, informados da indústria. Portanto, não estamos gerando nada novo aqui. Uma das preocupações em comum, é que nós estejamos gerando novos dados, que talvez não sejam exatos. Mas em múltiplas ocasiões, reiteramos que isso é o que os operadores de correio, prestadores de serviços de internet, utilizam diariamente. Não estamos criando nada novo aqui. Os critérios para incluir essas listas de bloqueios de reputação no sistema, tem que ter uma classificação de ameaça, que se condiga com as nossas próprias

ameaças de segurança. Tem que haver evidência de que essas comunidade de segurança e operacionais confiam nessas listas RBL para exatidão, qualidade, clareza do processo. Também tem que haver representações positivas e essas listas RBL devem ser amplamente aceitas pela comunidade de segurança operacional. Isso se demonstra , porque os dados são incluídos nas atividades de segurança comercial. E também, são conhecidos pelos operadores de network e pelos fornecedores de correio eletrônico para proteger seus usuários de todas essas questões. As RBLs, que utilizamos, tendem a bloquear mais que do o correio eletrônico comercial não solicitados, utilizam os navegadores. Um Google Chrome utiliza a APWG. Essa lista é utilizada também em sistemas, que fornecem conteúdo e também em sistemas de nuvem. Por exemplo, a Akamai utiliza SURBL, Amazon utiliza outro. Eu não lembro o que significa WAF. Utiliza isso para bloquear os ataques maliciosos e o RBL também bloqueia as palavras que não são boas. E também temos o DNS, que utiliza as zonas de políticas de recursos não nos resolutores. E há outros que fornecem RBL em formato RBC. Mais detalhes de como se utilizam essas listas de bloqueio. Não estamos aqui utilizando coisas, que sejam experimentais, é isso que queremos mostrar. É algo que já está sendo utilizado nos serviços comerciais em produção. Estivemos também trabalhando com os estudos acadêmicos para rever a informação e as práticas, que estão utilizando para ver como os

investigadores podem chegar, levar informação de confiança e uma série de estudos sobre os RBLs, que nós estamos utilizando para isso. Então, o conjunto de dados de RBL, que estamos utilizando agora são as listas de domínio apenas SURBL. Também a lista, que é chamada de SPAM house, o grupo de trabalho de phishing. Aqui a direita, tem uma lista composta do que é utilizado para identificar o software malicioso. o DAAR não identifica todos os tipos de abuso, não há nenhum fornecedor de reputação, que possa ver todos os tipos de abuso. Cada um tem a sua própria lista do abuso, que se produz na internet. Diferentes RBLs se focam em diferentes coisas específicas e é por isso, que nós fazemos essa acumulação de todas as RBLs. Porque queremos ter uma lista mais integrada de todas as coisas, que se veem na internet. Normalmente, recebemos uma pergunta e é: "Por que estamos informando os domínios que são SPAM no comunicado da reunião de Derabadi do GAC?". O GAC expressou o seu interesse em ter informação sobre os usos de SPAMs. E da nossa perspectiva, a maior parte do SPAM do correio não desejado, é enviado através de e-mails dobrados ou ilegais. Em geral, através de BOT nets. Já não se associa o SPAM com o conteúdo, que tem a ver com o correio eletrônico. A SPAM é termos de links, de twits, também facebook e outros sistemas de mensagens. E o SPAM é de fato, um dos meios principais através dos quais são implementadas outras ameaças. Esses, mencionados no comunicado do GAC da reunião de Beijing.

Vemos, então, o SPAM, como um serviço na nuvem. O caso da BOT net de avalanche, por exemplo, deu registro de domínio a seus clientes para fazer a transmissão de SPAM. DAAR, o que nós usamos em DAAR, são nomes de domínios que são encontrados no corpo das mensagens de SPAM. Ou seja, aqueles onde as pessoas fazem click para poder mandar a descarga do e-mail malicioso. O mais importante é que a reputação do domínio de SPAM, influi em quão agressivamente os administradores de correio eletrônico de segurança, aplicam filtros. Vimos que os administradores do sistema, se focam primeiro no SPAM. Porque é um indicador muito bom dos domínios comprometidos. Nós, agora, no sistema DAAR, que já está na etapa de produção, estamos utilizando... faz tempo, que estamos utilizando a nível interno, não publicamos relatórios que geram o DAAR. Porque queremos fazer as coisas bem e não rápido. Então, o que temos é uma revisão de um terceiro independente, da metodologia do DAAR para reunir dados. E essas revisões... uma acaba de terminar ontem e a segunda vai terminar em alguns dias. E vamos, então, passar essas informações a comunidade. E se esses relatórios dão alguma sugestão de mudança, é claro que vamos implementar essa mudança. Se a nossa intenção é que essas revisões nos ajudem a passar o SSAC. Para que o SSAC diga o que temos que fazer com a metodologia utilizada para o DAAR. Nesse momento, os informes, as informações internas com esses gráficos que

aparecem aqui, são apenas internas. O nosso objetivo, nesse momento, é que comecem a ficar a disposição para comunidade. Para, então, em termos de política, antes da reunião do Panam sobre o que tem a ver com o uso indevido do DNS. Vocês podem ver que todos os gTLDs tem pelo menos, um nome de domínio onde se registrou um abuso. Há diferentes cores, podem ver, para ter uma ideia aqui, como foi reportado esse uso indevido e como mudou através do tempo. Claro que o SPAM é o líder, mas também encontramos phishing, malware e BOT nets. Dentro do OCTO, nós pegamos essas informações que geram o DAAR e fazemos esse gráficos e se tivéssemos animação, veriam como sobem e descem essas borbulhas do quadro. Como crescem e diminuem. Mas assim aparece na tela fixa e se mostra que os domínios com phishing são os mais comuns. Em termos gerais são os maiores domínios. Mas é uma banda relativamente limitada. Também, começamos ver algumas coisas, que fogem do reino da estatística normal. A nossa intenção no futuro é que vamos publicar os nomes para dar as pessoas uma ideia do que são os registros e os registradores que sofrem mais abusos. Próximo slide, por favor. Claramente, o SPAM é uma coisa muito interessante. Especialmente, porque varia com o tempo. Aí, vocês podem ver essas borbulhas como sobem e descem, vão de direita à esquerda. É muito interessante ver tudo isso. Porque dá uma informação importante sobre o que nós chamamos de flocking.

É unificar e passar, então, em grupo de um registrador a outro. É o que acontece com a resolução de nomes entre os legados dos nomes de TLDs. Vemos que os legados tem uns números conhecido, já. E também, acontece a mesma coisa com os novos de gTLDs e que tem a ver com a registração total e abusos. Aqui aparecem os abusos de domínios, que estão no DAAR. Aqui vemos um aumento no caso dos legados através do tempo e uma diminuição nos novos gTLDs. Uma das coisas que tem o DAAR e se alguém estiver interessado no uso indevido, dá uma grande quantidade de dados para dizer: "Bom, o que está acontecendo aqui, o que entretém aqui a minha equipe?". Porque não queremos que as pessoas saiam pela rua e façam o que fazem, geralmente, a noite. Então, queremos ver, como prevenir. Então, aqui, temos essas estatísticas que demonstram que há uma quantidade relativamente pequena de domínios, que são os que geram a maior quantidade de abusos. É uma coisa, já conhecida há algum tempo. Mas DAAR está passando dados específicos ao respeito. Aqui está o estado do projeto, como já mencionei, nós estamos nos concentrando em fazer alguma coisa boa. Mas não rápido, como já falei, temos também, informações dos revisores, que são aqueles que vão aparecer essa semana. Estamos ajustando os sistemas de recuperação de dados para gerar, então, umas atualizações que sejam flexíveis e oportunas. A ideia é poder automatizar grande parte do relatório para não ter, então, mão-de-obra manual.

Fazer tudo de maneira oportuna, como dividimos esses dados que obtemos. Estamos experimentando com algumas informações específicas. Bom, com isto. Eu termino.

Há uma área que apresenta mais desafios , que tem a ver com o DAAR e se relaciona a reunião de informação sobre os registradores, que é uma função do "who is". E agora, não temos muita certeza, não confiamos muito sobre os dados dos registradores. Como para publicá-los nas primeiras versões. Depois, talvez, possamos publicar essa informação. Mas ainda devemos pensar exatamente, como podemos recuperar os dados dos registradores e que sejam eficazes. Com isso, eu termino. Passo a palavra para Fabien. Não sei se há alguma pergunta.

LAUREEN KAPIN: Obrigado por essa apresentação, David. E realmente, agradecemos como a ICANN está realizando este esforço. Esta informação, para nós, será importantíssima. Especialmente, porque tem a ver com desenvolvimento governamental de políticas. Porque coloca sobre o microscópio, quais são os problemas. A atenção que temos que dar. O desenvolvimento de políticas. Se temos que mudar os procedimentos, se temos que melhorá-los. Para poder ter uma forma de combater este tipo de abuso sistêmico, que acontece. Gostaríamos de escutar o que é

que deveríamos fazer antes de que esta iniciativa esteja em condições de dar informações públicas para ver onde está esse abuso, esse uso indevido. Quanto a determinação de domínios registradores e registros.

DAVID CONRAD: Como eu já disse, o centro, o foco nosso. O foco antes de publicar os nomes vinculados com os dados, que aparecem é ter uma revisão independente por parte de um terceiro, para verificar que não estamos fazendo nada injusto com os dados, para minimizar a chance de erro. De que existam informações falsas, que exista também, uma má atribuição de dados, no que tem a ver com o abuso do DNS e tentar levar o nível de confiança à comunidade de que os dados que nós estamos dando, podem ser utilizados para ter informação específica concreta para fazer um desenvolvimento de políticas. Quando os revisores terminarem o seu trabalho, como eu já falei, vai acabar, eu acho que daqui há alguns dias ou semanas estará pronto. Aí vamos poder apresentar esses relatórios ou informações. E vamos começar, então, com o processo que tem vinculação com a geração dos relatórios para publicá-los. A fim de que a comunidade se beneficie deles, mencionando quais são as estatísticas reais, onde estão os atores dentro dessas estatísticas.

LAUREEN KAPIN: Falaram também do rate limited, da limitação na velocidade. Eu não sei se entendi bem o que significa.

DAVID CONRAD: Bom, nos serviços das redes, pode existir uma denegação de serviços. Para isso, para iniciar, então, uma recuperação de dados, mais rápido do que pode fazer esse sistema. Então, os operadores das redes e de serviços impõem uma limitação, para reduzirem a quantidade de conexões que podem acontecer para evitar o uso indevido. No contexto dos registros e registradores. Na verdade, eu acho que todos eles tem limitações de velocidade. Porque, então, as pessoas não podem ir buscar em todas as bases de dados, para buscar os contatos que geraram o SPMA ou outro tipo de ataques. O efeito colateral é que os pesquisadores que estão tentando compilar informações para atribuírem, então, os nomes de domínios aos registradores. Significa que temos que enfrentar esses limites na quantidade de conexões. Às vezes, podemos fazer apenas 5 consultas por hora. Uma coisa assim. Esses são os limites estabelecidos. Então os fundamentos para estas limitações obviamente tem a ver com uma coisa razoável, com uma coisa prudente para as operações da rede. Seria bom encontrarmos a forma, de que os pesquisadores reconhecidos ou credenciados estejam numa

lista sem esses impedimentos ou limitações. Mas estamos lutando com isso, por enquanto.

CATHRIN BAUER BULST: Muito obrigado, David, por essa informação. Quero destacar o que tem a ver com a responsabilidade dos atores individuais, porque eu acho que houve uma reclamação específica sobre um registrador em especial, que em termos diplomático sofreu, estava sujeito a uma grande quantidade de abusos. Então, na reclamação se dizia que tinha base no relatório DAAR. Estamos falando em Janeiro de 2017, ou seja, não tinha base nos dados recentes. Esse é um ponto onde os relatórios DAAR vão ter valor. Porque vão dar, então, informação sobre uma análise contínua do abuso, que também vai estar vinculado a atores específicos e vai permitir, então, a transparência que esperamos para poderem suplementar os esforços de complemento contratual. Eu acho que estamos ficando sem tempo. Mas não sei se alguém tem uma outra pergunta, antes de encerrar esta sessão.

LAUREEN KAPIN: Eu tenho uma última pergunta. Eu suponho que os senhores sabem que podem existir mudanças no sistema do "who is". E o que eu quero saber é: "Como essas mudanças podem afetar a iniciativa DAAR?"

DAVID CONRAD: O sistema DAAR em si, não utiliza informações de identificação pessoal. A única identificação e informação utiliza a DAAR dentro da ICANN, o que é pertinente para a informação da qual estamos falando e ao do registrador e do nome de domínio social. Então, as outras informações são úteis quando a pessoa tenta aprofundar e entender um ataque em especial, um vetor em especial. Mas para fins de gerar o relatório, a informação do registrador é a única que nos preocupa na verdade. Na teoria, pelo menos, essa informação deveria estar disponível no "who is" público. Sem qualquer limitação para o seu acesso. Sabemos que há debates no momento, que tem a ver com a decisão final sobre que informação estará disponível para o público e qual não. Mas este tema ainda está pendente.

LAUREEN KAPIN: Obrigado. Então... Obrigado, Oliver, por todos os esforços, iniciativas. Porque eu sei, também, que vai ser de benefício para a comunidade. Eu sei que é muito trabalho. Então, queremos agradecer todo esse trabalho. Vamos encerrar a parte primeira deste debate do PSWG, que falou sobre o nosso plano de trabalho e fizemos um centro especial dessa.. uma das iniciativas, que tem a ICANN e vai ajudar a dar mais luz a este tema do abuso do DNS. Ver também, quais são as tendências

para que a comunidade incorpore estes dados no desenvolvimento de políticas. Estamos encerrando este tema, então. E agora, rapidamente...