ICANN77 | Fórum de políticas – Discussão do GAC sobre abusos do DNS e novas tecnologias
Quarta-feira, 14 de junho de 2023 – 10h45 às 12h15 DCA

JULIA CHARVOLEN: Olá, e bem-vindos à reunião do GAC sobre mitigação de abuso de DNS. Essa sessão está sendo gravada e regida pelos padrões de comportamento esperados da ICANN. Os comentários e perguntas deverão ser colocadas no chat, digitadas no formato correto. Diga o seu nome e o idioma que falará, se não falar em inglês. Fale de forma clara, e para permitir uma boa interpretação, não esqueça de silenciar todos os outros dispositivos. Passo a palavra ao presidente do GAC, Nicolás Caballero.

NICOLÁS CABALLERO: Muito obrigado. Nós teremos Susan Chalmers do Departamento de Comércio dos EUA, NTIA. Teremos Karel Douglas, do ministério de Telecomunicações de Trinidad e Tobago, também copresidente do Grupo de Trabalho de Regiões Desfavorecidas. Também teremos Lorraine Kapin, da Comissão Federal de Comércio dos Estados Unidos, também copresidente do Grupo de Trabalho de Segurança Pública do GAC, e Chris Lewis-Evans, da Agência Nacional do Crime do Reino Unido, copresidente, aliás, do GAC Public Grupo de Trabalho de Segurança. Também teremos como palestrantes convidados Russ Weinstein, e espero estar pronunciando bem o sobrenome, da ICANN Global Domains and Strategy, e Peter Jansen da EURid. Então sejam

todos bem-vindos. Próximo slide, por favor. Vamos dar uma olhada na agenda de hoje. Portanto, o primeiro tópico será uma visão geral das propostas de alteração do contrato de abuso de DNS e das ameaças à segurança do DNS com as quais elas foram projetadas para lidar. Então teremos o EURid falando sobre.eu e abuso de DNS e assim por diante. O terceiro tópico será o Workshop de Desenvolvimento de Capacidade do GAC do Dia Zero sobre abuso de DNS e, para isso, provavelmente darei a palavra a Karel e à equipe do Grupo de Trabalho de Regiões Desfavorecidas. E, finalmente, teremos uma discussão do GAC para determinar as próximas etapas. Então, com isso, bem-vindos a todos novamente e deixem-me passar a palavra ao Chris. Cris, por favor, vá em frente.

CHRIS LEWIS-EVANS: Muito obrigado, Nico, e Chris Lewis-Evans pelo registro. Então, na verdade, vou passar para Russ para nos dar um esboço rápido das alterações contratuais e, depois disso, examinarei o que isso realmente significa em um mecanismo de segurança pública. Então, Russ, para você. Muito obrigado.

RUSSELL WEINSTEIN: Claro. Obrigado, Chris, e obrigado a todos por me receberem. Meu nome é Russ Weinstein. Sou vice-presidente de contas e serviços da ICANN em nossa equipe de domínios e estratégias globais, e isso significa que gerencio todos os nossos relacionamentos e administração de contratos com nossos registros e registradores. Também sou responsável por coordenar o programa interno de

mitigação de ameaças à segurança do DNS da ICANN, portanto, este projeto relacionado a emendas contratuais para abuso de DNS se encaixa em ambas as funções e estou feliz por estar aqui e obrigado por nos receber hoje. Tão importante lembrar antes de entrarmos no que o contrato muda, quais são as mudanças, de onde isso veio e qual é o contexto por trás disso. Todos vocês sabem que o abuso de DNS tem sido um tópico de grande interesse e discussão por muitos anos na comunidade da ICANN, e houve um grande progresso ao longo do caminho nos últimos anos, especialmente muito trabalho voluntário e trabalho de melhores práticas produzido em a comunidade, principalmente nas partes contratadas, mas havia claramente a necessidade de mais. E no outono deste ano passado, as partes contratadas se reuniram e apresentaram uma proposta à ICANN e a toda a comunidade de que podemos fazer algumas mudanças importantes no contrato, limitando essas mudanças, com foco na criação de uma obrigação de mitigar e interromper abuso de DNS e, em seguida, permitir que a comunidade da ICANN tenha discussões sobre o que mais deve ser feito quando se trata de abuso de DNS em um formato de desenvolvimento de política aberta, e fazendo isso de maneira focada e produtiva, mas começando com as emendas contratuais focadas limitadas. E foi isso que nos esforçamos para fazer. Esforçar-se para criar emendas contratuais que criem uma obrigação significativa e executável para todos os registros e registradores de mitigar ou interromper o abuso de DNS quando for evidente em suas zonas. Então, veremos o que são essas emendas contratuais. E a ideia aqui é criar um piso, um novo piso para os cartórios e registradores que tenham essa obrigação.

Próximo slide. Portanto, um resumo de alto nível, e já apresentamos isso em alguns lugares, então esperamos que você tenha tido a chance de conferir a sessão da semana de preparação que fizemos algumas semanas atrás, ou a sessão que tivemos ontem, ou se alguns de vocês estiveram em nossa discussão na segunda-feira, ou no domingo com alguns dos membros do GAC também. Mas as mudanças em poucas palavras são que começamos com as obrigações existentes no contrato de registro e registrador, e não há nada que seja retirado dessas obrigações existentes. Nós apenas adicionamos em cima para aqueles. Portanto, nessas alterações, esclarecemos que os contatos de abuso para cada registro e registrador precisam estar prontamente disponíveis e acessíveis nas páginas da Web e melhoramos alguns aspectos com a denúncia de abuso de DNS. Portanto, adicionamos a capacidade de registros e registradores de utilizar um formulário da Web para coletar relatórios de abuso de DNS em vez de endereços de e-mail, como sabemos e aprendemos ao longo dos anos, publicar um endereço de e-mail na Web torna-se apenas uma fonte de spam, complica e coloca barreiras ao bom trabalho que os registros e registradores estão fazendo, tentando encontrar as verdadeiras reclamações de abuso e tomar providências enquanto lidam com a filtragem. Também adicionamos o recurso em que os registros e registradores agora precisam confirmar o recebimento de uma denúncia de abuso. E isso ajuda o reclamante, o registrador e a ICANN em situações em que o escalonamento é necessário ou um acompanhamento adicional é necessário.

Essas emendas adicionam uma definição de abuso de DNS para o propósito desses acordos, e nós começamos, e vamos nos aprofundar

nisso. E então, como mencionamos, cria uma nova obrigação de agir e mitigar, parar ou interromper o abuso de DNS em cada um dos contratos.

E junto com essas mudanças nos contratos, as mudanças nos contratos são realmente apenas alguns parágrafos para cada um dos contratos. Mas adicionamos um rascunho de aviso que também faz parte do documento de apoio com o comentário público. E esse comunicado tem cerca de 15 páginas e explica o que esses requisitos significam com mais profundidade e clareza, como seria a aplicação e como a implementação deveria ser em alguns casos.

Há vários exemplos lá que você pode seguir. Eu realmente encorajaria todos os interessados neste tópico a ler esse aviso. É uma leitura fácil, mas um documento complementar realmente útil. Próximo. Então, vou entrar nos dois tipos de obrigações principais aqui. Portanto, o primeiro começa com a adição de uma definição de abuso de DNS, e adicionamos isso aos contratos de registro e registrador. E, para fins desses acordos, abuso de DNS significa malware, botnets, phishing, farm e spam quando usados como vetor para fornecer outras formas de abuso de DNS. Essas definições vêm do trabalho que vem sendo feito na comunidade da ICANN há algum tempo. Nós liberamos várias dessas coisas de volta ao SAC 115 como uma fonte de bom trabalho vindo da comunidade. Essas são coisas que, olhando em toda a comunidade, há um consenso claro de que tudo isso é abuso de DNS, e há pouca ou nenhuma dúvida de que essas coisas são abuso de DNS. E essa é a nossa base inicial quando falamos sobre o que essas obrigações são relativas. Próximo slide. Portanto, sabendo o que é abuso de DNS, as principais

obrigações do contrato de registrador são: quando um registrador tem evidências acionáveis de que um nome registrado patrocinado por um registrador está sendo usado para abuso de DNS, o registrador deve tomar imediatamente as medidas de mitigação apropriadas que são razoavelmente necessárias para impedir ou impedir que esse nome seja usado para abuso de DNS.

E uma coisa importante a ser lembrada com relação ao abuso de DNS é altamente contextual e, portanto, nem todos os casos de abuso de DNS têm a mesma abordagem de mitigação e o mesmo resultado esperado. Mas todas as ações de mitigação necessárias devem se concentrar em tentar impedir ou impedir que esse nome seja usado para abuso de DNS. Isso é uma grande melhoria para onde estamos hoje. Próximo slide. Da mesma forma, do lado do registro, é quase a mesma obrigação, mas tem alguma consideração pela função do registro versus a função do registrador. Pensamos no registrador como o mais próximo do cliente do nome registrado e, muitas vezes, em uma posição diferente para interagir com esse cliente para resolver problemas de abuso. Portanto, o registro tem, como eu disse, quase a mesma obrigação, mas eles têm, no mínimo, que a ação atenuante seja o encaminhamento do caso junto com qualquer evidência acionável ao registrador, o que então chutaria sua obrigação, a obrigação do registrador de que que acabamos de discutir, ou tomar essa ação atenuante por conta própria para interromper ou interromper o abuso de DNS por conta própria e ter a capacidade de fazer qualquer uma dessas coisas, mas exigir que eles façam uma dessas coisas é um grande problema novamente para registros. Portanto, essas são as principais

obrigações nos acordos. E acho que estou passando de volta para Chris ou há mais perguntas ou estamos quebrando para perguntas?

CHRIS LEWIS-EVANS: Então, Russ, acho que se eu pudesse fazer meus dois slides e depois fazer perguntas, se for Nico. Brilhante, obrigado. Então, Chris, vamos estabelecer o recorde. Então, o que eu queria abordar era, na verdade, como parte dessa linguagem afeta o que estamos vendo do ponto de vista da segurança pública e como isso nos permite agir? Como isso permite que os registros e registradores ajam com base nas evidências que podemos fornecer a eles? E realmente cobre tudo? Isso nos dá as ferramentas de que precisamos para tomar as medidas apropriadas? E durante o workshop de desenvolvimento de capacidade, ouvimos perguntas sobre, bem, isso cobre phishing por SMS? cobre isso? cobre isso? E eu tenho dois, três, quatro exemplos aqui de, na verdade, sim. Portanto, no lado esquerdo, há uma captura de tela de uma mensagem SMS dizendo que a conta de alguém precisa ser atualizada ou suspensa é normalmente o idioma que aparece. E então tem um link para alguém clicar que inclui o nome do domínio. Isso é phishing, abuso de DNS todos os dias.

Então, junto com uma captura de tela talvez do site ao qual está vinculado, para mostrar que não é o site real do provedor de celular, seria uma inteligência acionável, seria capaz de fornecer alguma prova de dano se tivéssemos uma reclamação de que isso rouba senhas e assume contas. Isso nos permite dizer, aqui está, isso é um phishing, abuso de DNS. E a linguagem então diz que eles devem agir prontamente porque têm evidências acionáveis e tomar a ação

apropriada. Portanto, neste caso, se for um domínio registrado com códigos maliciosos, eles seriam capazes de suspender esse domínio e isso seria necessário. Eles também podem recomendar que entremos em contato com o host e removamos o conteúdo, mas essa seria uma etapa de mitigação apropriada. Então sim, está coberto. Se você receber a mesma coisa por e-mail, sim, está coberto. Desde que tenha o nome de domínio no qual você precisa clicar. Também ouvimos falar de domínios parecidos, então aqueles que dependem talvez de um pequeno erro de digitação ou aqueles que apenas adicionam uma palavra extra para fazer você pensar que é legítimo. Portanto, o exemplo à direita é um desses. E aparece um serviço que provavelmente muitas pessoas usam. E depende de você fazer isso, seja uma das plataformas de mídia social ou seja uma entrega de pacote que todos recebem de um dos varejistas. Oh, eu só preciso fazer o login. E então ele irá capturar suas senhas e tudo mais e então utilizar isso para atividades criminosas. Isso é coberto? É sim. Portanto, acho muito bom que haja alguma clareza nessas alterações para identificar alguns desses itens de phishing que são cobertos. E o PSWG disse, certamente no ICANN 76, obteve os números da maneira errada. Uma grande proporção da atividade criminosa vista é baseada em ataques de phishing. Portanto, poder ter vários tipos de phishing vinculados a esse idioma é muito importante para podermos agir contra isso. Passe para o próximo slide, por favor. Brilhante, obrigado. Portanto, a coisa mais importante para muitos governos no momento é o ransomware.

O ransomware é coberto por isso? Não é mencionado. Mas o ransomware é uma forma de malware. Então sim, é. Se houver um domínio que está distribuindo malware que criptografa o dispositivo de

alguém ou tudo mais, isso está coberto? É sim. Essa é uma das áreas-chave que conheço para muitos governos no momento em relação ao risco, tanto para entidades comerciais em seus países, mas também para infraestrutura nacional crítica. Então isso está coberto. Excelente. Então, o spyware que é colocado nos dispositivos das pessoas está coberto? Sim, é outra forma de malware. Algumas pessoas também dizem Trojans. Então, algo que você acha que é realista, mas também rouba seus dados. Isso é apenas outra forma de malware. Isso também seria coberto pela legislação se estiver vinculado a um nome de domínio. Adware, novamente, clica em um domínio, diz para você baixar algo, você acha que é real, isso é malware, está distribuindo malware. Está coberto? É sim. Então, realmente, muitas das ameaças que vemos que entregam criminosos ou permitem que criminosos causem impacto nas vítimas, tudo isso está coberto na definição que foi usada. Então, do nosso ponto de vista, este é realmente um bom passo à frente no que temos. Isso torna, para os registradores, muito mais claro sobre o que eles devem agir ou o que devem agir usando o idioma. Então eu acho que é realmente um bom passo à frente e uma boa elevação real do piso. E com isso, gostaria de abrir para perguntas. Obrigado.

NICOLÁS CABALLERO: Obrigado. Muito obrigado, Chris. Então, antes de passar a palavra para Peter Janssen e passarmos para os próximos tópicos, que você leu, é assim que se diz? Alguma pergunta, algum comentário, alguma reação na sala ou online? Gulten?

GULTEN TEPE: Obrigado, Nico. Temos Ken-Ying Tsang de Taipei Chinês e depois Kavouss Arasteh da delegação do Irã.

NICOLÁS CABALLERO: Taipei Chinês, por favor, continue.

KEN-YING TSENG: Obrigado, presidente. Só para constar, meu nome é Ken-Ying. Eu sou do Taiwan Network Information Centre. Sou um representante do GAC de Taipei Chinês. No que diz respeito à emenda aos acordos sobre abuso de DNS, acredito que a linguagem cuidadosamente redigida em um equilíbrio muito delicado na forma como existem algumas normas e impedimentos para que qualquer uma das partes tenha certa discrição para interpretar no futuro.

Esta deve ser uma boa maneira de devolver a flexibilidade, o que também mostra a importância do aviso, que acredito servirá como uma referência para todas as partes para implementar no futuro cláusulas contratuais relacionadas ao abuso de DNS. Mas eu tenho algumas perguntas sobre a interpretação do idioma. Em primeiro lugar, vi as palavras razoavelmente ou razoável mostrando o idioma tantas vezes. Só estou me perguntando se a interpretação dessa razoabilidade deve ser da perspectiva do registrador ou registro ou da ICANN, quando a ICANN conduz auditoria de conformidade. Essa é a minha primeira pergunta. E a minha segunda pergunta é sobre questões transfronteiriças. Acredito que, para situações de abuso de DNS, muitas vezes o abusador e o denunciante e o registrador ou registro provavelmente estariam em pelo menos três jurisdições diferentes. Só

estou me perguntando se as obrigações que impomos aos registradores ou registros, nós consideramos a natureza transfronteiriça do incidente, idioma potencial ou barreiras culturais? Obrigado.

NICOLÁS CABALLER: Chris, você gostaria de prosseguir?

CHRIS LEWIS-EVANS: Talvez se Russ responder à primeira, eu possa cobrir a segunda.

RUSSELL WEINSTEIN: Parece bom. Obrigado, Cris. Aqui é Russ Weinstein da ICANN. Obrigado por sua pergunta. Portanto, a primeira pergunta foi sobre razoabilidade e acho que quem é o árbitro da razoabilidade. Então eu acho que a forma de interpretar que é primeiro a obrigação do contratado é que ele se comporte de forma razoável. E então, se isso for questionado, a ICANN avaliará a razoabilidade dessas escolhas e fará sua própria determinação se foi razoável ou não, e faremos isso com base em nossa experiência, muitos anos de experiência neste campo e também nossa experiência com estas disposições contratuais. E então acho que a ICANN tem a discrição de que precisamos para fazer cumprir esses contratos é a parte principal.

CHRIS LEWIS-EVANS: Obrigado, Russ. E para o segundo ponto em torno das fronteiras cruzadas. Então você está certo, você provavelmente terá três

jurisdições se tiver sorte, talvez cinco ou seis que eu vi, definitivamente em vários casos. A linguagem aqui não permite que a polícia simplesmente entre e diga que você deve fazer isso por meio de um pedido. Existe um processo para isso, um sistema judicial, MLAs, tudo mais. No entanto, o que ele faz é permitir que as solicitações internacionais de registradores examinem as evidências que você está fornecendo e, em seguida, tomem as medidas apropriadas com base no que determinam essas evidências. E eu sei que falando com registradores e registros, eles sempre apreciam muito as boas evidências que as autoridades podem fornecer. Estamos bastante acostumados a fornecer pacotes de evidências.

Então, quando fornecemos isso, geralmente é bem recebido e começa a conversa sobre se você realmente tem algo um pouco mais e seríamos capazes de tomar essa ação. Portanto, a linguagem definitivamente permite uma ação transfronteiriça. Não é um que eles vão agir sobre isso. Será uma determinação baseada nas evidências. Obrigado.

NICOLÁS CABALLERO: Obrigado, Chris. Em seguida, tenho o Irã. Por favor, vá em frente.

KAVOUSS ARASTEH: Muito obrigado, Chris. Obrigado a todos. Acho que, se me permite, Chris, dois casos exatamente aconteceram comigo. Há alguns meses, recebi uma mensagem do Secretário-Geral da UIT de manhã cedo, nove horas, por favor, venha imediatamente ao meu escritório. Então eu me preparei para ir e então eu chequei. Descobri que não vem do Secretário Geral da UIT, Sr. Zhao. Que tipo de abuso é esse? A segunda, recebi

outra mensagem chamada Christina e algo assim. Achei que é uma daquelas Christina que está trabalhando nos grupos de trabalho da ICANN. Eu respondi a isso. Ele disse, por favor, reconheça este e-mail. Então descobri que não é a Christina que conheço. É alguma coisa de Christina. Não sei. Que categoria de abuso é esse e a quem devo denunciar ou não devo denunciar nada? No entanto, eu imediatamente, em dois minutos, mudei minha senha imediatamente. Obrigado.

LAUREEN KAPIN: Kavouss, esses são realmente ótimos exemplos porque nos mostram a gama de comunicações que ao longo do espectro podem ser irritantes, irritantes, até o abuso, que pode ter danos reais acionáveis em termos de consequências econômicas, etc. et cetera, até mesmo consequências emocionais no caso de, por exemplo, golpes românticos. Mas, em relação a isso, não acho que chegariam ao nível do que chamamos de abuso de DNS porque não houve realmente um dano, embora houvesse irritação. O que vou apontar para as pessoas, assim como todos nós estamos interessados em nos proteger, às vezes até mesmo essas comunicações inócuas que você pode obter via texto, algo tão simples como um oi pode ser o primeiro passo para algo que se torna mais perigoso, talvez um golpe de impostor. Portanto, é bom excluir esses e-mails e não seguir o caminho de talvez divulgar informações confidenciais ou permitir que alguém acesse o computador porque acha que eles vão ajudá-lo com algum problema técnico. Mas para essas situações específicas, não chegaria ao nível de abuso formal de DNS, embora seja irritante.

NICOLÁS CABALLERO: Muito obrigado, Laureen. Eu tenho a Malásia a seguir. Sr. Mohamed Afiq. Vá em frente, por favor.

MOHAMAD AFIQ: Sim, obrigado, Nico, Afiq, pelo relatório. Em primeiro lugar, devo dizer que esta emenda é uma excelente iniciativa e já é hora de mitigarmos melhor o abuso do DNS no ecossistema do DNS. Então, a esse respeito, observei os documentos de alterações e não tenho certeza se existem outros documentos ou disposições que cobrem o mesmo. Mas eu me pergunto, no caso de discrepância na avaliação do registrador, do operador de registro ou talvez da unidade de conformidade contratual, quero perguntar, há alguma determinação para finalizar ou concluir a decisão que seria tomada sobre o nome de domínio em disputa?

NICOLÁS CABALLERO: Obrigado, Malásia. Gostaria de ir em frente, Russ?

RUSSELL WEINSTEIN: Claro. Aqui é Russ, para o registro. Estou tentando analisar um pouco a questão. Você se importaria de reafirmá-lo?

MOHAMAD AFIQ: Se houver alguma discrepância na avaliação quando a avaliação for feita pelo registrador ou pelo operador de registro, eles terão contradições ao concluir se o nome de domínio é realmente usado para abuso de DNS ou não. Então, se houver alguma contradição entre o

registrador e o operador de registro ou talvez a unidade de conformidade contratual, existe alguma determinação que possamos tomar para concluir a decisão que seria tomada sobre o próprio nome de domínio?

RUSSELL WEINSTEIN: Ótimo. Obrigado. Este é Russ novamente. Portanto, se você, como reclamante, enviar suas evidências ao registrador, acreditar ter um caso válido de phishing ou uma das outras formas de abuso de DNS e receber uma resposta de que eles não acham que foi abuso de DNS, você deve leve isso ao nosso departamento de conformidade contratual, e nós levaremos isso para eles. Faremos nossa avaliação de sua reclamação, garantiremos que seja válida e que tenhamos as evidências de que precisamos. Também temos a capacidade de validar se algo está sendo usado para abuso de DNS e, se descobrirmos isso, levaremos ao registrador e trabalharemos para obter a retificação. Então, acho que isso aborda sua preocupação.

MOHAMAD AFIQ: Obrigado.

NICOLÁS CABALLERO: Vá em frente, Sr. Afiq. Vá em frente.

MOHAMAD AFIQ: Então você está dizendo que a unidade de conformidade contratual aqui terá a palavra final ou talvez aquela que determina se há um abuso

de DNS sendo conduzido por meio desse DNS, por meio desse nome de domínio?

RUSSELL WEINSTEIN: Portanto, o compliance da ICANN terá a capacidade de apresentar nossa visão à parte contratada com nossa determinação. O contratado terá a oportunidade de apresentar seu ponto de vista e perceber se nós estávamos certos ou eles estavam certos. Há também a possibilidade nesta discussão de que a ação que a parte contratada tomou pode não corresponder à sua expectativa, mas pode ser que a parte contratada tenha tomado medidas razoáveis, e se você for ler o aviso, há várias seções lá sobre o diferenças entre tipos de abuso de DNS e nomes de domínio particularmente comprometidos em que suspender o nome de domínio nem sempre seria a ação apropriada e, portanto, eles podem seguir outro caminho para resolver isso, e pode ser por isso que você está se sentindo insatisfeito, e esses casos não implica necessariamente em mudança de rumo por parte do contratado. Esperançosamente, isso amarra isso.

NICOLÁS CABALLERO: Obrigado, Russ. Com licença. Obrigado, Malásia. Em seguida, tenho o Japão. Nobu, por favor, vá em frente.

NOBUHISA NISHIGATA: Obrigado, Presidente, e obrigado a todos. Japão, em primeiro lugar, deixe-me dizer que apreciamos muito todo o esforço para chegar ao projeto de emenda, e tenho um esclarecimento a pedir. A questão é, o

contrato atual antes da alteração, o contrato atual não proíbe as partes contratadas de tomar ações voluntárias contra atividades maliciosas ou ilegais se necessário, envolvendo o uso dos nomes de domínio. E então a pergunta, o pano de fundo é como Russ disse, às vezes o curso de ação da vítima das más atividades maliciosas ou ilegais, mas a reação do registro de risco nem sempre atende à expectativa, assim como você mencionou, e então vemos alguma frustração nas indústrias japonesas. Dito isso, apreciamos que esta alteração ajude as partes contratadas a impedir ou interromper o uso de nomes de domínio gTLD por abuso de DNS. Obrigado por perguntar. Deixe-me pedir um esclarecimento. Obrigado.

NICOLÁS CABALLERO: Obrigado, Japão. Chris ou Russo?

RUSSELL WEINSTEIN: Obrigado. Peço desculpas. Estou tendo problemas para detectar qual era a parte da pergunta.

NICOLÁS CABALLERO: Você poderia repetir a pergunta?

NOBUHISA NISHIGATA: Então, se você olhar para o rascunho da emenda, e então temos um bom texto, como as partes do contrato devem tomar alguma ação, mas sem esse texto no contrato atual, mas as partes do contrato podem tomar ação necessária, se considerada necessária, para fazer algumas

ações de forma voluntária, na medida em que derrubem os servidores, se necessário. Apesar de estar em abuso de DNS ou não, conforme definido no SAC 115.

RUSSELL WEINSTEIN: Então, o que esta emenda faz é codificar o que é abuso de DNS como essas cinco coisas e quais são os requisitos para mitigar e parar ou interromper esse abuso de DNS. Os contratos existentes, você está certo, usam um pouco de abuso, e isso continuará a ser uma provisão nesses contratos para um conjunto mais amplo de coisas, e o registrador tem mais liberdade de como lidar com isso. Eles ainda têm que lidar com isso. Eles têm que investigar e responder, mas respondem de forma adequada e dentro de suas atribuições.

NOBUHISA NISHIGATA: E quanto ao lado do registro? Temos o contrato existente. Temos o ponto de partida que podemos a vítima pode, ou talvez como os advogados podem enviar inquérito, então o cartório recebe o inquérito, depois o cartório, se eles acharem necessário ou urgente, esse tipo de julgamento, então eles podem tomar a ação voluntária contra essas coisas ruins relatadas.

RUSSELL WEINSTEIN: Não há nada nos contratos que proíba os registros e registradores de tomar medidas que considerem adequadas.

NOBUHISA NISHIGATA: Muito obrigado.

NICOLÁS CABALLERO: Obrigado, Japão. Obrigado, Russ. Eu tenho a República Democrática do Congo, Blaise. Vá em frente, por favor.

BLAISE AZITEMINA FUNDJI: Obrigado, Presidente. Em primeiro lugar, gostaria de agradecer ao Chris por levar em consideração um assunto que estávamos discutindo no domingo, se bem me lembro. E no ambiente móvel que você trouxe, ou agora é considerado claramente como uma questão de abuso de DNS, porque isso preocupava a maioria dos países da região subdesenvolvidos ou mal atendidos. Muito obrigado por isso. Acho que estamos avançando. Mas agora eu tenho uma pergunta, acho que um comentário. Na maioria das vezes, com provedores de serviços de Internet, temos um problema, não é realmente malicioso, mas não sei se isso se enquadra nas condições gerais ou é uma desculpa para ISPs nas condições gerais.

Eles inscrevem os usuários à força em alguns serviços nos quais os usuários não se inscrevem voluntariamente. Mas você acaba descobrindo em sua conta que assinou, ou foi cortado, ou foi cobrado por uma certa quantia de dinheiro pelo uso do serviço A ou serviço B. Por que você não se lembra de ter assinado pessoalmente esse tipo de serviço. Mas quando você entra em contato com os provedores, eles dizem que isso se enquadra nas condições gerais. Claro, eles não são maliciosos para serem considerados phishing ou não, mas isso não é

feito com a vontade dos usuários. Então, como você considera isso? Obrigado.

CHRIS LEWIS-EVANS: Sim, então Chris Lewis-Evans para registro. Isso provavelmente se enquadraria no spam, mas dentro da definição de abuso de DNS, como você disse, não está entregando nenhuma das outras atividades maliciosas, portanto não se enquadraria no abuso de DNS. Portanto, seria mais um problema de proteção de dados, pelo que você está dizendo, relacionado aos ISPs, do que um problema de abuso de DNS.

LAUREEN KAPIN: E brevemente, Blaise, isso soa como uma questão de proteção ao consumidor sobre cobrança não autorizada. Portanto, não necessariamente algo que caia no abuso de DNS, mas certamente uma questão importante. As pessoas não devem ser cobradas por coisas sem saber.

NICOLÁS CABALLERO: Obrigado, Laureen. E eu passo a palavra para a Comissão Européia, Gemma, e então precisamos seguir em frente.

GEMMA CAROLILLO: Muito obrigada.

NICOLÁS CABALLERO: Gemma, vá em frente.

GEMMA CAROLILLO: Obrigada. Muito obrigado, presidente, e tentarei ser muito breve e aproveitar também o que alguns colegas disseram, em particular um colega do Japão. Então, em primeiro lugar, estamos muito felizes em ver isso se movendo. Este é um desenvolvimento crítico. E o sucesso dessa iniciativa vai ser muito importante para o funcionamento geral do modelo da ICANN, se você quiser, pela forma como toda a comunidade pode se unir e fazer algo importante. E por isso também queremos contribuir construtivamente nesta sessão. E nós participamos da capacitação no domingo, e vamos participar dos comentários do público, então faça o nosso melhor para contribuir de forma construtiva. E deixe-me mencionar apenas duas, três coisas, que também compartilhamos com os colegas na capacitação.

Uma é a que o Japão estava se referindo. Portanto, dada a essência da velocidade no combate ao abuso de DNS, o que é enfatizado no comunicado para que os registros e os registradores possam monitorar proativamente o abuso de DNS, para nós é realmente essencial. Acreditamos que existem muitas boas práticas na indústria. Preferimos ver isso embutido, se possível, nos contratos, mas para consideração de qualquer maneira. O segundo ponto é que valorizamos muito a assessoria complementando os contratos. É muito útil. Mas seria importante, nos contratos ou separadamente, garantir que as disposições relativas à execução sejam claras. Porque isso é importante para a conformidade da ICANN e é importante para todas as partes interessadas que fique claro quais são as consequências da não conformidade. E, por último, há uma parte importante sobre

transparência nos contratos, portanto, registros e registradores prestam contas sobre relatórios sobre ações de abuso de DNS. E também achamos que seria importante aumentar o nível de transparência para que haja clareza sobre quais são as políticas sobre abuso de DNS que as operadoras estão adotando e relatórios sobre o curso de ação. Então você relata, essa é a quantidade de abuso que temos reagido dessa forma ou de outra, porque isso também ajuda a entender como os contratos, que são, claro, de alto nível, são implementados na prática. Muito obrigado.

RUSSELL WEINSTEIN: Muito obrigado, Gemma e Chris, isso serve para o registro. Portanto, o monitoramento proativo é uma daquelas coisas bastante difíceis de fazer. Então, eu sugeriria que talvez para o próximo estágio de contratos, ou se há estruturas voluntárias sobre como os registradores e registros podem fazer isso, seria um bom comentário a ser considerado na próxima vez. Sobre a clareza sobre o que a conformidade pode fazer, acho que provavelmente é um bom comentário para fazermos como GAC sobre como podemos garantir que o comunicado reflita o que Russ disse hoje, que a conformidade pode tomar medidas para garantir que a comunidade esteja Ciente daquilo. Então, nesses dois pontos, eles são meu reflexo. Obrigado.

CHRIS LEWIS-EVANS: Obrigado por seus comentários. E só para complementar o que Chris disse, espero que esteja claro nessas emendas e por meio do comunicado, mas ouvi dizer que pode haver alguma falta de clareza

nisso, que a conformidade tem a discrição e a capacidade de ir até o fim violar, rescindir essencialmente um contrato de registro ou registrador se encontrarmos violações ao agir de acordo com esses requisitos. Então isso deve ficar claro. Isso foi discutido o tempo todo com os contratantes, é isso que estamos tentando fazer. Estamos tentando levantar a palavra e garantir que todos estejam fazendo isso para proteger a indústria, para ter uma indústria limpa. Portanto, não deve haver equívoco de que este não é um acordo executável que apresentamos aqui para você.

NICOLÁS CABALLERO: Muito obrigado, Chris. Obrigado, Russ. Obrigado, Comissão Europeia. E por questão de tempo, não aceitarei mais perguntas. E vamos para o próximo tópico. Peter Janssen, a palavra é sua.

PETER JANSSEN: Obrigado. Bom Dia a todos. Vejo que meus slides já estão prontos. Meu nome é Peter Janssen. Sou o gerente geral da EURid. Essa é a organização sem fins lucrativos com sede na Bélgica que gerencia o domínio de nível superior.eu, domínio de nível superior com código de país. E para o registro,. eu e suas três escritas diferentes, latim, grego e cirílico, respectivamente, para dar suporte a todos os idiomas falados na União Européia. N a apresentação de hoje, tentarei fornecer uma visão geral da mitigação e prevenção do abuso de DNS que nós, como registro, adotamos. E já peço desculpas na frente. Este é um assunto que levaria facilmente várias horas para entrar em qualquer tipo de profundidade. Vou tentar ser o mais breve possível. Quem me conhece sabe que falo

demais e falo rápido demais. Então, peço desculpas novamente ao pessoal da tradução que é muito difícil para eles. Então, obrigado por me apoiar lá. Próximo slide, por favor. Para lhe dar uma ideia do que vou falar, fiz uma pequena visão geral do que chamo de processo de registro e delegação. Portanto, como você deve saber, existem diferentes atores nesse processo de aquisição de um nome de domínio.

No canto superior esquerdo, você tem o registrante, o futuro detentor do nome de domínio, que de alguma forma, e essa é a seta com o número um, entra em contato com um registrador que usa algumas das interfaces do registro, e essa é a seta número dois, para realmente transmitir essa solicitação do registrante para ter um nome de domínio registrado. Uma vez que o registro, neste caso, seu ID, recebe essa solicitação do registrador, uma série de verificações e balanços são feitos, que é a seta número três. Por exemplo, para.eu, existem certos critérios de elegibilidade que devem ser cumpridos. O registrante precisa ter um endereço de residência na União Europeia ou em qualquer um dos estados do EEE, ou ter cidadania em qualquer um desses estados membros ou estados do EEE. Isso é verificado pelo registro de maneira totalmente automática. Uma vez que todos esses freios e contrapesos estejam bem, o número quatro, na verdade, há outra pessoa aqui. Então, o número quatro realmente resulta em que o nome de domínio seja registrado e salvo no banco de dados de registro. É o que chamamos de processo de registro. Obviamente, há muito mais detalhes do que isso, mas essa é a funcionalidade de alto nível do que o registro de um nome de domínio realmente envolve. Depois que um nome de domínio é registrado, as pessoas podem acessar nosso site, acessar a interface UIS e realmente ver que esse nome de domínio está

registrado e não pode mais ser registrado por mais ninguém, obviamente.

Mas isso não significa que esse nome de domínio realmente funcione na internet, que é a segunda parte desse processo, que é o processo de delegação. Então, à direita, e agora as setas mudam para amarelo e usam letras em vez de dígitos para fazer a distinção, existe o que chamamos de processo de delegação de nome de domínio, que extrairá todas as informações relacionadas ao DNS do banco de dados de registro, que em termos técnicos é o próprio nome de domínio, o serviço de nome e qualquer tipo de material de chave DNSSEC relacionado a esse nome de domínio e o inserirá no que chamamos tecnicamente de arquivo de zona. Então, novamente, temos. eu em latim. eu em grego e.eu em cirílico, por isso mantemos três arquivos de zona que correspondem a esses três scripts. O processo de delegação de nome de domínio injetará isso nesse arquivo de zona, e é tarefa do servidor de nomes primário garantir que tudo em um nível técnico esteja correto e enviará essas informações aos servidores de nomes secundários que ficam ao redor do mundo, o que realmente fará o nome de domínio funcionar, pelo menos a parte pela qual o TLD é responsável, que é a primeira parte do processo de resolução. Não vou entrar em detalhes aí, porque aí a gente estaria aqui ainda amanhã, eu acho. Então esse é o processo de registro versus delegação. Próximo slide, por favor.

Se você observar o processo de delegação de nomes de domínio em sua forma mais simples, ele realmente extrairá essas informações do banco de dados de registro e as alimentará nos arquivos de zona que o

servidor de nomes primário, como você viu no slide anterior, propagará para o serviço de nome secundário, serviço de nome oficial no mundo. O que fazemos é realmente adicionar funcionalidade a esse processo de delegação de nome de domínio que, uma vez que o processo de delegação de nome de domínio deseja realmente delegar esse nome de domínio, ele perguntará o que chamamos de mecanismo de decisão.

NICOLÁS CABALLERO: Peter? Desculpa por interromper. Você precisa desacelerar um pouco. Sinto muito por isso, mas vá em frente, vá em frente. Mas desacelere um pouco.

PETER JANSSEN: Sim, esperado. Eu novamente peço desculpas. Então vou tentar ser mais lento. Funcionará por 10 segundos, provavelmente. Portanto, o processo de delegação de nomes de domínio normalmente extrai as informações do banco de dados de registro, insere-as no arquivo de zona e sua tarefa é concluída. O que fizemos foi adicionar funcionalidade a esse processo de delegação de nome de domínio. E, na verdade, no momento da delegação, ele perguntará ao mecanismo de decisão, como o chamamos, devo realmente delegar esse nome de domínio? E esse mecanismo de decisão determinará com base nos atributos de um nome de domínio, e voltarei a isso em um slide, se esse nome de domínio foi registrado com potencial intenção maliciosa. Então, ele tentará prever esse nome de domínio, é um registro de nome de domínio malicioso, sim ou não? Darei um pouco mais de detalhes nos próximos slides sobre isso. Se o mecanismo de decisão decidir que

sim, este é um registro potencialmente malicioso, isso atrasará a delegação. O que isso significa?

Ele não irá inseri-lo no arquivo de zona. Então, tecnicamente, o nome de domínio é registrado, então ninguém mais pode registrá-lo. Mas ele não funciona na Internet, portanto, nenhum abuso de DNS pode realmente acontecer com esse nome de domínio. Em segundo lugar, iniciamos o que chamamos de processo de validação, onde solicitaremos ao registrante que realmente valide os dados do registrante. Obviamente, como você pode imaginar, se for uma entidade maliciosa que deseja registrar um nome de domínio com intenção maliciosa, essa validação não acontecerá pela simples razão de que essa pessoa ou entidade não quer ser descoberta. E naquele momento, com a falta dessa validação bem-sucedida do registrante, basicamente suspendemos e retiramos o nome de domínio depois de um tempo. Se o mecanismo de decisão disser não, está tudo bem, não parece suspeito, sem trocadilhos, obviamente o nome de domínio será delegado como tal. Próximo slide, por favor. Para esse mecanismo de decisão, alguns de vocês já devem ter ouvido falar do acrônimo APEWS.

E nós amamos nossas siglas. Todas as duas, três e quatro letras são tiradas, então fomos para o acrônimo de cinco letras. APEWS significa Abuse Prediction and Early Warning System, e seu objetivo é realmente, no momento do registro de um nome de domínio, prever se esse nome de domínio está registrado com intenção maliciosa ou abusiva. Ele faz isso construindo um número ou treinando vários modelos de aprendizado de máquina que se baseiam nos atributos de um nome de domínio. Quais são os atributos práticos que levamos em conta?

Obviamente, os dados do registrante, o nome, o endereço, o e-mail, o número de telefone e assim por diante. O registrador em questão que realmente registrou um nome de domínio. Algo que chamamos de aleatoriedade do nome de domínio. Nós, como humanos, detectamos com muita facilidade que um Q7499P7-3 parece bastante aleatório para nós, então isso pode ser estranho. Então essa é uma das coisas que toca também. E então, obviamente, as informações de DNS, os servidores de nomes também são levados em consideração. Próximo slide, por favor.

Então, como isso funciona? Esse modelo preditivo, por um lado, pega uma lista de nomes de domínio abusivos conhecidos por feeds de segurança de terceiros, nomes que foram usados em estado selvagem para enviar spam, fazer ataques de phishing e esse tipo de coisa. Por outro lado, os dados de registro de nomes de domínio correspondentes a esses nomes, mas também muitos nomes que são nomes de domínio genuínos de boa-fé que não são abusivos. Essas informações são alimentadas em um processo de treinamento automático diário que, por fim, fornece um preditor, um preditor de aprendizado de máquina. Esse preditor vai, no momento da delegação, pegar as informações sobre o novo registro e fazer uma previsão se aquele nome de domínio está potencialmente registrado com intenção maliciosa, sim ou não. Então você pode se perguntar, está tudo bem. Estamos tentando prever se um nome de domínio é com más intenções, sim ou não.

Quão bom ou quão ruim é isso? Próximo slide. O que você vê aqui é um gráfico onde no eixo x, então o eixo horizontal, você vê o início de 2018. E no lado direito, você vê janeiro um pouco mais longe, 2023, bem

recente. E no eixo y, ou seja, no eixo vertical, você vê o número de nomes de domínio registrados mensalmente, pelo menos uma porcentagem que está sendo sinalizada por nosso sistema APU como potencialmente maliciosa. Então o 0,02 que você vê aqui significa 2%. Há uma série de coisas que você pode concluir a partir deste gráfico. Primeiro, a esmagadora maioria de todos os nomes de domínio é sinalizada como genuína, genuína, sem problemas, sem nada. Portanto, o nome de domínio é delegado como de costume e não há danos. Não há nenhum problema. Em segundo lugar, se você olhar para 2018 a 2019, verá uma queda bastante grande no número de nomes de domínio que realmente são sinalizados como maliciosos ou potencialmente maliciosos. Isso pode significar várias coisas. Isso pode significar que os bandidos estão ficando melhores em escapar do nosso radar. Ou, e isso é o que provamos, é que não, nosso sistema realmente desencorajou vários atores mal-intencionados a fazer o caminho de vários registros que faziam no passado.

Portanto, nosso sistema realmente mostra que, ao implementar isso, e é um sistema totalmente automático, vários registros abusivos desapareceram com o tempo. Com o tempo, você vê vários picos. Nós investigamos essas coisas, e algumas delas são na verdade tentativas de maus atores para contornar nossos mecanismos, e é uma espécie de galinha e, não, galinha e ovos, jogo de gato e rato, onde sempre adaptaremos nossos sistemas para evitar o atores mal-intencionados evitem nossos sistemas e assim por diante. Próximo slide, por favor. Portanto, o modelo de previsão, como é típico do aprendizado de máquina, precisa ser ajustado, e há dois termos interessantes para falar aqui. Há muito mais, mas vou me concentrar apenas em dois. Um é

chamado de recall, que significa essencialmente quantas das coisas que você está procurando você realmente encontrou? E o outro é a precisão. Daqueles que você estava encontrando, quantos estavam realmente corretos? Então, em nossos termos, isso significa que o nome de domínio foi marcado como um registro malicioso. Foi realmente um registro malicioso? Sim ou não? Como podemos saber? Fizemos isso executando o sistema no início sem agir nas decisões.

Portanto, tínhamos o sistema funcionando em tempo real e, quando o sistema previu um registro de nome de domínio malicioso, não interrompemos a delegação. Nós apenas deixamos passar e, na verdade, verificamos mais tarde se esse nome de domínio foi realmente usado para fins maliciosos. Sim ou não? E como você pode ver, tanto o recall quanto a precisão, em nossa experiência, ficaram acima de 80%. O que isso significa, uma precisão de 80%? Que em quatro dos cinco casos em que um nome de domínio é sinalizado como malicioso, mais tarde apareceu nos feeds de segurança que foi realmente usado para uma tentativa de phishing ou qualquer um dos abusos de DNS mencionados na apresentação anterior. A desvantagem típica do aprendizado de máquina é que você não pode ter tudo. Você não pode ter uma recordação perfeita e uma precisão perfeita. É uma escolha, e é para isso que estamos ajustando nosso modelo.

E aqui estamos tentando ser o mais seguros possível, no sentido de que, se sinalizarmos um nome de domínio como malicioso, queremos ter certeza de que realmente foi um registro malicioso. Portanto, otimizamos a precisão, mesmo ao nível em que alguns dos registros maliciosos não são encontrados. Mas se sinalizarmos um nome de

domínio como malicioso, mas ele for realmente registrado por um usuário normal da Internet para fins normais, quais são as coisas ruins que acontecem aqui? Isso é o que chamamos de falso positivo. Portanto, é previsto como malicioso, mas é realmente benigno. Nesse caso, como você viu no slide anterior, o registrante é convidado a validar os dados do registrante. Temos vários mecanismos baseados em EID, pagamentos bancários e esse tipo de coisa que permite ao registrante verificar com muita facilidade os dados do registrante.

Portanto, mesmo no caso de falsos positivos, não é a pior coisa que pode acontecer ao registrante. É um processo muito simples do que seguir os movimentos e provar que você é quem disse que era. Próximo slide, por favor. Então, onde você pode usar essa coisa? Temos isso no que chamamos de configuração de pré-delegação pós-registro. O sistema entra em ação depois que o nome de domínio é registrado, mas antes que o nome de domínio seja potencialmente implantado no arquivo de zona, o que significa que, se não delegarmos, o nome de domínio não poderá ser usado. Então o abuso não é realmente possível, o que é bom. Outra possibilidade seria, na verdade, fazer o pré-cadastro. Portanto, não permita o registro se a previsão for de que o registro do nome de domínio seria um registro malicioso. Em primeiro lugar, seu sistema teria que ser rápido o suficiente para realmente ser capaz de fazer isso. Mas, em segundo lugar, existe o risco de que, se você tiver um falso positivo em que está dizendo que o registro de nome de domínio seria malicioso, então você não permite o registro, você está basicamente impedindo o princípio do primeiro a chegar, primeiro a servir, daí a razão pela qual decidimos deixar o registro passar. Mas

antes que o nome de domínio seja ativado, faça a pré-delegação para realmente fazer essas verificações.

Outra possibilidade é o pós-registro, pós-delegação. Portanto, para todos os nomes de domínio normais que estão no banco de dados de registro, você pode usar este sistema para detectar se algum desses nomes de domínio que potencialmente foram registrados há 10, 20 anos, se são maliciosos, sim ou não. Mas, naquele momento, há uma grande quantidade de outras informações disponíveis que tornam muito mais fácil ver se um nome de domínio é malicioso, sim ou não. O conteúdo dos sites é obviamente um exemplo lá. E, por último, um projeto muito interessante que estamos analisando são os TLDs cruzados. Vemos padrões abusivos semelhantes em diferentes extensões. Então, estamos falando aqui hoje sobre. eu e seus três scripts, mas tudo ainda com o mesmo registro. Mas o que vemos é que os mesmos atores mal-intencionados também registram registros maliciosos em outras extensões. Portanto, seria interessante ver que tipo de inteligência, que tipo de informação e que tipo de ganho pode ser encontrado ao juntar essas informações. E é exatamente isso que estamos fazendo neste momento. Estamos trabalhando com outros ccTLDs na Europa para realmente criar um sistema conjunto em que as informações de registro desses diferentes registros sejam alimentadas em um sistema central para poder detectar melhor esses padrões abusivos.

Obviamente, naquele momento, um aspecto que vem à tona é o GDPR, privacidade de dados, porque naquele momento, você está realmente alimentando um sistema com dados cadastrais de diferentes

jurisdições e diferentes registros. E isso é algo que resolvemos anonimizando os dados do registrador. E eu dou um exemplo aí. Meu nome, Peter Janssen, está mapeado em uma técnica chamada MD5 hash. Não significa nada para os humanos. O que é importante notar aqui, é uma maneira. De Peter Janssen para aquela sequência de aparência aleatória é fácil. Voltar é quase impossível. E, na verdade, o que é interessante é que, ao contrário dos humanos, os modelos de aprendizado de máquina não se importam se é Peter Janssen ou se é C103CE e assim por diante. Ele só quer ver certos padrões. E estou chegando ao fim para aqueles que estão me pressionando para calar a boca agora. Acho que estamos no último slide de qualquer maneira. Então, o que estamos fazendo aqui é ver se podemos tornar isso ainda melhor no reconhecimento de padrões abusivos, passando por diferentes TLDs sem passar por obstáculos especiais em informações relacionadas à privacidade. Porque, basicamente, as informações que alimentamos no sistema são aleatórias no que diz respeito aos seres humanos. Próximo slide, por favor. Acho que estava no final do slide. Então, obrigado por sua atenção. Se houver alguma dúvida, ficarei feliz em tentar respondê-la.

NICOLÁS CABALLERO: Muito obrigado, Pedro. Isso é realmente fascinante. Desculpe interrompê-lo, mas por uma questão de tempo, acho que poderemos responder a apenas duas ou três perguntas no máximo, e temos que garantir que alocaremos tempo suficiente para a reunião de Hamburgo. Desculpe por isso, Pedro. Muito obrigado por essa explicação detalhada. Temos alguma pergunta rápida ou comentário na sala ou na

sala de bate-papo? E não vejo nenhum. Então, com isso, de volta para você. É Susan ou Karel? Karel, me desculpe. Desculpe. Karel, vá em frente, por favor.

KAREL DOUGLAS: Obrigado, Nico. Aqui é Karel Douglas, Trinidad e Tobago GAC. E muito obrigado pelo seu convite aqui. Sei que ainda temos alguns minutos, então serei breve. Eu tinha algumas anotações, mas acho que seria mais fácil para mim falar de cabeça. Então, voltando, o slide ou a foto à sua frente daria uma ideia do que tivemos no dia 11 de junho, que foi o nosso dia de capacitação. A razão pela qual temos este dia de capacitação é realmente permitir que as pessoas que são novas no GAC, e talvez aquelas que não são tão novas, saibam quais são os problemas e sejam capazes de entender os problemas e contribuir com eles, e realmente ter o maior número possível de pessoas contribuindo. Portanto, neste dia em particular, nos concentramos nos problemas de abuso de DNS. Então, duas questões que eu quero dizer. O abuso de DNS é um deles, e também o processo de comentários públicos. Portanto, o processo de comentários públicos, é claro, é o processo de consulta empregado quando consideramos os problemas. Portanto, era importante para nós garantir que os membros do GAC entendessem o processo de comentários públicos e as etapas tomadas a esse respeito. E também, a questão do abuso de DNS. E tivemos apresentações fantásticas da comunidade. E devo dizer que tivemos apresentações fantásticas sobre o processo. E para combinar essas duas questões, essas questões críticas, decidimos ter sessões de grupo em que os participantes foram divididos em diferentes grupos por

idioma. Então tínhamos cinco grupos, e era francês, espanhol, árabe, chinês e inglês. Isso é importante. E a ideia era que as pessoas agora tivessem a oportunidade de discutir entre si nos grupos linguísticos questões que lhes são pertinentes. Então, saindo disso, e sei que estamos com pouco tempo, tivemos voluntários. A entrega crítica foi o fato de que agora temos cinco pessoas que se ofereceram para ajudar no processo de comentários públicos sobre abuso de DNS. E nós, é claro, nesses grupos de discussão, algumas coisas que foram discutidas foram o processo em si e também as questões de abuso de DNS. Então, essas mesmas duas questões. E posso apenas seguir para uma das perguntas que foram feitas sobre as definições. E esse foi um tópico no qual passamos algum tempo por causa da questão da razoabilidade e rapidez e um tanto vago, mas entendemos ou exploramos o problema e sabemos que esses problemas tendem a ser definidos na circunstância específica. Então, obviamente, quando se trata de um cenário de vida ou morte, o tempo razoável ou razoável pode ser de segundos, enquanto que quando não é de vida ou morte, pode ser de semanas, conforme o caso.

Portanto, isso explicaria por que, em alguns casos, as definições são interpretadas de forma ampla, de modo que se apliquem de acordo com o caso, conforme o caso. Esta imagem antes de você, meu último ponto, é na verdade a sessão de breakout. Temos Nigel, vejo lá, no grupo de inglês. Isso é basicamente o que tivemos alguns dias atrás e essas conversas. E esperamos que isso transcenda a um documento e nossas contribuições sobre a questão do abuso de DNS no contrato. Futuro, e vou terminar com isso, o workshop de capacitação é realizado pelo grupo de trabalho de regiões carentes. Sou um dos copresidentes

junto com Paul Hunter e temos o apoio de Tracy Hackshaw e outros. Neste caso, certamente, o governo dos EUA, Susan Chalmers. Portanto, certamente queremos ter outros no futuro, não apenas sobre abuso de DNS, mas outros. E é realmente trazer todo mundo para o grupo para que você se sinta à vontade para fazer suas contribuições. Então, muito obrigado e desculpe se passei por isso.

NICOLÁS CABALLERO: Muito obrigado, Karel. Infelizmente, não poderemos responder a perguntas neste momento, então eu passo a palavra para Susan Chalmers dos Estados Unidos. Susana, por favor, vá em frente.

SUSAN CHALMERS: Muito obrigada, presidente. Então serei breve. A ICANN abriu um processo de comentários públicos sobre as alterações contratuais propostas e os comentários devem ser enviados até 13 de julho. Esta data está chegando e temos um cronograma ambicioso, como vocês podem ver aqui, para preparar a contribuição do GAC.

Portanto, o processo deve ser mais ou menos assim. Em primeiro lugar e imediatamente, a partir de hoje, vamos solicitar comentários dos membros e observadores do GAC sobre um Documento Google que conterá perguntas de orientação, às quais procuramos chegar hoje, mas, infelizmente, acredito que estamos sem tempo por isso.

O pequeno grupo, os voluntários que Karel mencionou, e obrigado a esses voluntários, desenvolverá um primeiro rascunho com base nessas informações e, simplesmente, o rascunho será distribuído ao

GAC. O pequeno grupo revisará e julgará a entrada e as linhas vermelhas e distribuirá um documento para consenso até 13 de julho. Resumindo, agradecemos a participação de todos os representantes do GAC. Junte-se a nós para contribuir com a contribuição do GAC para o importante trabalho da comunidade nessa questão.

NICOLÁS CABALLERO: Muito obrigado, Estados Unidos. Laureen, gostaria de acrescentar algo?

LAUREEN KAPIN: Claro. Microfone. Sim, se pudermos ir para o próximo slide. Estamos sem tempo, mas Nico gentilmente concedeu uma pequena janela de cinco minutos apenas para que todos pudéssemos dizer, plante sementes. Não teremos todos os brotos e flores agora, mas teremos tempo durante a redação do comunicado do GAC para também discutir isso mais a fundo. Então, essas são as sementes que quero plantar para você pensar. Considerações para o processo de comentários públicos.

Quais são, na sua opinião, os aspectos positivos destas alterações? Acho que já houve uma boa discussão sobre isso. A questão da aplicabilidade. É ótimo ter uma linguagem, mas a borracha pega a estrada onde é exequível, então considere essa linguagem e sua aplicabilidade. Considerações sobre a definição proposta de abuso de DNS, e isso é como os três ursos, Cachinhos Dourados e os três ursos. Muito largo, muito estreito, suficientemente flexível, perfeito. Considerações sobre a função do consultor da ICANN sobre a emenda, porque isso fornece algumas informações de orientação realmente boas que podem ser vistas como um documento que evoluirá à medida

que a conformidade ganhar mais experiência com esses cenários e considerar o que pode ser útil em termos de orientação e é suficientemente informativo quanto a alguns desses termos que já foram discutidos, como razoável, como pronto, como acionável e caminhos de escalonamento. Quem é responsável por fazer o quê?

O que faz sentido nas circunstâncias particulares? Próximo slide, desculpe se estou falando muito rápido para os intérpretes. Espero que não. E então, porque isso foi sinalizado como o primeiro de muitos passos neste tópico complicado e em evolução, a questão também é importante para pensar sobre o que vem a seguir, e uma ideia que foi discutida e acho que também endossada por muitas pessoas dentro do A comunidade da ICANN é a ideia de processos de desenvolvimento de políticas específicos e muito direcionados sobre questões muito específicas. Por exemplo, você pode ter um PDP sobre qual é a melhor maneira de lidar com phishing, por exemplo. Quais devem ser as respostas apropriadas? Isso serve de exemplo. Portanto, você pode considerar qual pode ser o assunto do futuro trabalho de política sobre abuso de DNS e também não apenas o que deveria ser, mas quando deveria ser? Deve ocorrer antes da próxima rodada de novos gTLDs ou não necessariamente? O papel do interesse público e os compromissos voluntários do registro, acabamos de ouvir sobre isso na discussão com o conselho.

A importante questão de como você lida com criminosos reincidentes, registrantes, registradores, registros que são paraísos para atividades ilícitas. Para os registrantes, é claro, podem ser os atores envolvidos em atividades ilícitas, e qual seria o momento ideal para essas questões?

Essa não é uma lista completa. Mais uma vez, são sementes para plantar em suas mentes, ideias para discussão adicional para o possível comentário público do GAC. Portanto, deixo para vocês pensarem bastante sobre isso e sei que todos se juntarão para garantir que a contribuição do GAC aqui seja tão forte e cuidadosa quanto possível.

NICOLÁS CABALLERO: Muito obrigado, Laureen, e obrigado a Susan, Carol, Chris, que não está mais aqui, e Russ e Peter. Certamente isso é algo para reflexão do GAC, mas precisamos encerrar a sessão. Alguma pergunta ou reação rápida? E precisamos ser muito rápidos. Caso contrário, a sessão é encerrada. Muito obrigado. Vamos adiar. E, na verdade, precisaremos parar por cerca de cinco minutos para reagendar. Rob, me corrija se eu estiver errado. Por favor, vá em frente.

GULTEN TEPE: Estamos prontos para continuar, Nico.

NICOLÁS CABALLERO: Nossa próxima sessão é sobre tecnologias emergentes. Os objetivos da sessão são basicamente criar uma lista de tópicos de tecnologia sobre os quais o GAC, o comitê, gostaria de aprender mais e sugerir prioridades e preferências. Esse é o primeiro. A segunda é identificar e discutir opções de estruturas informativas que o GAC poderia usar melhor para compartilhar informações ou conteúdo no futuro. E obrigado novamente. Obrigado novamente, Karel, Susan, Laureen.

Portanto, a ideia básica era criar uma lista de tópicos de tecnologia. O pano de fundo é que, ao planejar as discussões para a reunião pública da ICANN77, os membros do GAC expressaram o desejo de identificar e discutir tópicos envolvendo novas tecnologias que influenciarão ou impactarão o DNS e a Internet no futuro. Portanto, as sugestões de tópicos iniciais que temos até agora são três, rota alternativa de DNS, blockchains e inteligência artificial. E, novamente, a ideia aqui é identificar e discutir quaisquer outros tópicos adicionais. Entendo que temos algumas sugestões do Taipei Chinês. Ken-Ying, não sei se você gostaria de prosseguir agora. Você tem uma apresentação ou é apenas um briefing oral para o GAC? Como você gostaria de proceder?

KEN-YING TSENG: Obrigado, presidente. Posso apresentar brevemente meus pensamentos e a razão pela qual propus este tópico. Em primeiro lugar, acho que todos nesta sala já devem ter notado que as tecnologias emergentes se tornaram o assunto mais discutido nos últimos anos. Talvez nos últimos dois anos, Web3 e blockchain tenham sido muito populares. E a partir do final de 2022, o chat GPT se tornou muito popular e a inteligência artificial vem dominando toda a discussão sobre tecnologia ao redor do mundo. É por isso que estou propondo que o GAC e a ICANN considerem se essa tecnologia emergente afetaria de alguma forma o sistema DNS e se devemos examinar algum dos problemas. Por exemplo, para inteligência artificial, acho que a apresentação de Peter mostra um exemplo muito bom porque parece que a ICANN ou outras partes relacionadas já adotaram inteligência artificial no combate ao abuso de DNS. Então, acho que poderíamos

pensar mais a esse respeito, se a inteligência artificial influenciaria nossas ameaças de segurança cibernética ou também poderia ser o contrário. Isso pode nos ajudar a evitar problemas de segurança cibernética ou atividades de abuso de DNS. Esses são meus pensamentos originais. Obrigado.

NICOLÁS CABALLERO: Muito obrigado, Ken-Ying. Temos alguma pergunta? Algum comentário? Alguma reação ao briefing de Ken Ying? Passe para o próximo slide, Gulten. E eu entendo que isso é para Alisa. Júlia, vá em frente.

JULIA CHARVOLEN: Me desculpe. Sim, temos uma mão levantada de Kavouss Arasteh da delegação do Irã.

NICOLÁS CABALLERO: Irã, vá em frente. Mas, por favor, seja breve e direto ao ponto. Vá em frente, Irã. Irã, a palavra é sua. Irã, a palavra é sua. Você poderia por favor ir em frente?

JULIA CHARVOLEN: Agora temos Ana Neves da delegação de Portugal na linha.

KAVOUSS ARASTEH: Com licença. Você me ouve agora?

JULIA CHARVOLEN: Sim, podemos ouvi-lo agora, Kavouss.

KAVOUSS ARASTEH: Muito obrigado. Desculpe. Eu perguntei o que você quer dizer com DNS alternativo? Obrigado.

NICOLÁS CABALLERO: Ken-Ying, gostaria de responder a essa pergunta? Ele perguntou exatamente o que você quis dizer com DNS alternativo, certo? Essa era a pergunta.

KEN-YING TSENG: Obrigado, presidente. Acredito que DNS alternativo significa outro tipo de identificador da web que não é o identificador normal ao qual estamos acostumados, ou seja, por meio do sistema da ICANN. Acho que para Blockchain ou Web3, eles têm seu próprio identificador da web, que é semelhante ao nosso, nosso sistema atual com camadas, mas eles não passam por nosso registrador e pelos registros. Esse é o meu entendimento, mas talvez o outro representante do GAC ou qualquer outro participante aqui tenha um conhecimento mais amplo do que eu.

NICOLÁS CABALLERO: Muito obrigado, Taipei Chinês. Holanda, por favor, vá em frente, Alisa.

ALISA HEAVER: Obrigada. Sobre rota DNS alternativa ou sistemas de nomenclatura alternativos, eu meio que preparei três perguntas e, desculpe, eu vou?

NICOLÁS CABALLERO: Não, não, vá em frente, porque eu tinha Portugal. Desculpa, Portugal, não vi a tua mão, mas vamos em frente com a Holanda e depois passo-te a palavra. Desculpe por isso, eu não vi isso. Desculpe, vá em frente, Alisa.

ALISA HEAVER: Então, para a pergunta de Kavouss, talvez devêssemos ir, acredito que haja uma pergunta preparada em uma enquete. Espero que todos os membros do GAC estejam na sala do Zoom e possam responder à pergunta da enquete, e isso foi meio que indo em direção à pergunta de Kavouss. Que rota DNS alternativa ou sistemas de nomenclatura alternativos são? E obrigado. Existe a enquete.

NICOLÁS CABALLERO: Muito obrigado Holanda. Portugal, sinto muito. Vá em frente.

ANA NEVES: Sem problemas. Apenas esteja preparado para me ouvir em português, é claro. Eu vou falar em português. Eu gostaria de mencionar, bem, estou esperando que os outros usem fones de ouvido para a interpretação. Eu gostaria de apoiar, apoiar inteiramente, a intervenção de Taiwan, assim como a intervenção da Holanda. É fundamental ter qualquer tipo de capacitação para entender o impacto

das tecnologias emergentes no DNS. Vai ser muito interessante aqui, isso no GAC, e poder ou ter a possibilidade de perceber do que se trata esse impacto. Essas tecnologias emergentes são importantes. Precisamos entender o impacto no futuro e seria necessário ter essa discussão aqui no contexto das sessões do GAC.

NICOLÁS CABALLERO: Em seguida, tenho Nigel Hickson, do Reino Unido, e depois tenho a OMPI. Vá em frente Nigel.

NIGEL HICKSON: Sim, obrigado, Sr. Presidente. Bem, vou adiar apenas por um segundo para a Holanda, caso haja mais para Alisa compartilhar, depois de fazer a pesquisa.

ALISA HEAVER: Claro, feliz em continuar, mas não quero atrapalhar a intervenção de Brian aqui.

NICOLÁS CABALLERO: Não, você pode continuar, Holanda.

ALISA HEAVER: Já temos os resultados da primeira pergunta? E espero que as pessoas tenham preenchido antes de ouvir a pergunta de Kavouss. Então temos 53%, creio que estou lendo, que já ouviram falar e 47% não. E bem, se isso é principalmente respostas de membros do GAC, bem,

basicamente metade do GAC nunca ouviu falar disso. A segunda pergunta para a qual poderíamos ir. Como você está vendo, estou tentando construir algo.

NICOLÁS CABALLERO: O que está perfeitamente bem. Essa é a ideia de toda a sessão. Então vá em frente, Holanda.

ALISA HEAVER: Temos a segunda pergunta chegando?

JULIA CHARVOLEN: Aqui é Julia, da equipe de suporte do GAC. Nós temos a segunda pergunta.

ALISA HEAVER: Obrigada, Julia. Talvez nesse meio tempo, enquanto as pessoas estão respondendo à pergunta, possamos ir para a intervenção de Nigel ou Brian.

NICOLÁS CABALLERO: Obrigado Holanda. Brian, por favor, a palavra é sua.

BRIAN BECKHAM: Obrigado, presidente. Boa tarde, colegas. Brian Beckham da OMPI. Em relação a este tópico, gostaria de mencionar algumas coisas que acho que seriam de interesse. Neste outono, em setembro, teremos nossa

oitava conversa da OMPI sobre IP e tecnologias de fronteira. Temos uma divisão de tecnologias de ponta que analisa a interseção de IA e IP e discute alguns dos tópicos que estão sendo discutidos aqui. Temos em nosso site uma versão arquivada da sétima conversa, que foi especificamente focada em blockchain e NFTs e IoT e metaverso. Posso compartilhar links para aqueles que estão na lista do GAC. Em abril deste ano, a INTA, Associação Internacional de Marcas Registradas, produziu um white paper sobre NFTs, que incluía domínios Web3. Mais uma vez, posso compartilhar o link para isso na lista do GAC. Eu gostaria de ler uma das recomendações deste artigo da INTA. Ele diz que a confiança dos consumidores é necessária para que os nomes de domínio Web3 sejam adotados em massa por consumidores e proprietários de marcas. A INTA, em colaboração com a WIPO, poderia considerar o desenvolvimento de uma política global de resolução de disputas de marcas registradas semelhante à UDRP que pode ser adotada para os ecossistemas digitais emergentes de NFTs e o metaverso. Só para lembrar aos colegas, a OMPI foi solicitada por seus estados membros em 1998 a produzir uma recomendação para o problema da interseção de nomes de domínio e marcas registradas, frequentemente chamado de cybersquatting. O resultado desse processo foi a UDRP, que foi a primeira política de consenso da ICANN, e temos administrado esse processo desde então. Claro, você deve se lembrar de que há uma revisão de política planejada pela ICANN da UDRP, e fornecemos informações aos colegas sobre isso anteriormente. E, concretamente, gostaria de mencionar que ontem, na reunião do IPC, anunciamos que o Namebase, que é um dos operadores desses domínios raiz alternativos no protocolo Handshake,

está adotando voluntariamente o UDRP para disputas de marcas registradas nesse alternativo específico raiz. Portanto, achamos que é um desenvolvimento muito positivo para os proprietários de marcas e esperamos que seja útil para iniciar novas conversas a esse respeito. Obrigado.

NICOLÁS CABALLERO: Obrigado, Brian. Muito obrigado. Eu tenho o Reino Unido e depois a China. Vá em frente, por favor, Nigel.

NIGEL HICKSON: Sim, muito obrigado, Nigel Hickson do UK GAC. Apenas para enfatizar, eu acho, a importância desta sessão. Obviamente, não vamos cobrir todo o terreno esta manhã porque é quase hora do almoço. Mas acho que isso realmente, retomando os pontos que Taiwan e a Holanda fizeram, aponta para a necessidade de uma sessão mais longa em nosso próximo encontro em Hamburgo. E tenho certeza de que temos a responsabilidade como vice-presidentes e presidente e outros, é claro, de agendar isso se o GAT mais amplo achar que isso é apropriado. Eu acho que, em particular, essa área de raiz DNS alternativa e blockchains é muito importante. Obviamente, a inteligência artificial também é importante. Mas acho que os dois primeiros itens são mais, talvez, mais pertinentes para nós no momento, devido ao seu significado. E o que Brian Beckham disse e outros, eu acho, também deve ser levado em consideração. Obrigado.

NICOLÁS CABALLERO: Obrigado, Reino Unido. Eu tenho a China e depois voltaremos para a Holanda. E então, se tivermos mais tempo, sinto muito, Ola, mas é assim que as coisas são. China, por favor, vá em frente.

GUO FENG: Obrigado, presidente. Guo Feng da China, para o registro. Portanto, esta sessão, acho esta sessão interessante. Mas no que diz respeito à organização deste tipo de sessão, se vamos ter a mesma sessão adicional no futuro, talvez em Hamburgo, sugiro que talvez queiramos convidar alguns dos especialistas em TI ou pessoas de tecnologia para nossa sessão para explicar a tecnologia no que diz respeito a esses tópicos. Porque nós, como um GAG, a maioria de nós, eu acho, somos pessoas políticas. Portanto, talvez esta seja a minha sugestão neste momento. Obrigado.

NICOLÁS CABALLERO: Muito obrigado China. Bem notado. Mas a ideia no começo era identificar possíveis temas, desenvolver uma agenda razoável e depois ver se o GAG realmente quer seguir com isso ou não, porque no final depende de nós. Agora, se concordarmos com isso, podemos desenvolver algo um pouco mais estruturado. E desculpe a falta de tempo neste momento. Só temos mais cinco minutos. Holanda, vá em frente, por favor.

ALISA HEAVER: Obrigada. Bem, já perfeito. Os resultados estão em alta. Estou vendo muitos baixos, alguns médios e alguns altos. Então, a maioria das

pessoas diz que não sabe muito sobre isso. E poderíamos ir para o próximo slide. Sim. Bem, definitivamente não vou ler tudo neste slide, mas basicamente diz qual é a rota alternativa do DNS. E gostaria apenas de indicar aos meus colegas um relatório da Okta de abril de 2022. Achei que era um relatório muito bom e isso despertou meu interesse neste tópico.

E então eu preparei uma terceira pergunta. Você quer ter capacitação sobre este tema? Mas parece que já foi respondido por todas as intervenções, então fique à vontade para respondê-lo. Mas minha sugestão foi, bem, com isso, apresentar brevemente o tema e deixar que todos leiam sobre ele. E espero que a maioria dos meus colegas tenha lido este relatório antes da sessão e possamos nos aprofundar no assunto. E vou deixar com isso aqui.

NICOLÁS CABALLERO: Muito obrigado Holanda. Mais uma vez, tenho a Suíça. Jorge Cancio, por favor, seja breve e direto ao ponto, estamos ficando sem tempo. Vá em frente, Suíça.

JORGE CÂNCIO: Sim, Nico. Jorge Cancio, para que conste, muito breve. Caso o GAC esteja interessado em inteligência artificial, o que o Conselho da Europa e outros países estão fazendo, seu antecessor, Thomas Schneider, está presidindo o comitê correspondente no Conselho da Europa. Ele estaria interessado ou feliz em vir ao GAC em algum momento no futuro, se você tiver interesse. Obrigado.

NICOLÁS CABALLERO: Certamente. Isso seria incrível. Isso certamente seria bom. Então, com isso, mais alguma coisa a acrescentar, Holanda?

ALISA HEAVER: Bem, talvez uma última coisa é que ontem falei brevemente com John Crane, o CTO, e ele ficaria mais do que feliz em nos ajudar com o workshop de capacitação. Então eu acho que isso é uma boa notícia. E espero que todos compareçam. Obrigado.

NICOLÁS CABALLERO: Obrigado Holanda. E, finalmente, tenho meu distinto vice-presidente, Ola Bergström, da Suécia. A palavra é sua.

OLA BERGSTRÖM: Obrigado, Nico. Então, acho que cobrimos a primeira parte agora sobre os tópicos. Acho que há muitos tópicos interessantes que precisamos explorar. Você pode ter o próximo slide. Acho que agora vou entrar no como, que também é uma questão muito complexa, é claro. Acho que temos muitas opções de abordagens diferentes, ferramentas diferentes, com que frequência devemos fazer isso e também o que já temos e nosso tipo de opção. Acho que precisamos ter uma discussão sobre o que caberia. Não acho que precisaríamos encontrar uma solução que se encaixasse em todos. Então, acho que precisamos de uma abordagem flexível para ter diferentes tipos de ferramentas e abordagens para atender a toda a comunidade do GAC. E estamos

definitivamente interessados em sua opinião, mas não temos tempo para aprofundar essa questão no momento. Mas voltaremos a isso.

NICOLÁS CABALLERO: Com certeza. Muito obrigado, Ola. Alguma pergunta final? Algum comentário final? Alguma reação na sala ou online? Gulten? Júlia? Não? Nada nada?

GULTEN TEPE: Recebemos uma ligação da delegação chinesa.

NICOLÁS CABALLERO: China, vá em frente.

GUO FENG: Obrigado, presidente. Na verdade, gostaria de voltar um pouco aos tópicos que talvez identificamos inicialmente em relação a esta sessão. Acredito que o segundo tópico seja sobre blockchain, mas talvez eu queira adicionar o elemento NFT. Talvez alguns de vocês saibam disso. É um token não fungível. Acho que é baseado no blockchain e talvez seja um identificador particular porque o DNS é um sistema de identificação. Acho que o NFT é o caso específico que talvez queiramos examinar. Obrigado.

NICOLÁS CABALLERO: Muito obrigado, China. Nós certamente vamos agregar o NFT à lista. Bom, temos mais um último comentário e feedback? Se não, então,

agradeço muito, em todos os idiomas, e voltamos às 13:45 horário local, muito obrigado.