
ICANN70 | Fórum virtual da comunidade – Grupo de Trabalho de Segurança Pública do GAC (PSWG)
Terça-feira, 23 de março de 2021 – 10h30 às 11h EST

GULTEN TEPE:

Bem-vindos à sessão do GAC da reunião de ICANN-70 de 23 de março. Não vamos nomear todos os assistentes, mas eles vão ser incluídos no anexo ao comunicado. Devo lembrar aos representantes em o atendimento para indicar presença atualizando o nome do participante para refletir seu nome completo e afiliação. Se você gostaria de fazer uma pergunta ou um comentário, digite-o iniciando e terminando sua frase com “Question” ou “Comment”, para permitir que todos os participantes vejam sua solicitação. A interpretação para as sessões do GAC inclui até 6 idiomas da ONU e português. Os participantes podem selecionar o idioma que desejam falar ou ouvir. Seu microfone ficará mudo durante a sessão, a menos que você entre na fila para falar. Se desejar falar, levante a mão na sala do Zoom. Ao falar, diga o seu nome para registro e o idioma que você falará, caso fale um idioma diferente do inglês. Fale claramente e em um ritmo razoável para permitir uma interpretação precisa e certifique-se de silenciar todos os outros dispositivos. Por fim, a sessão, como todas as outras atividades da ICANN, é regida pelos Padrões de comportamento esperados da ICANN. Você encontrará o link no chat para sua referência. Com isso, gostaria de passar a palavra ao presidente do GAC, Manal Ismail. É com você, Manal.

Observação: O conteúdo deste documento é produto resultante da transcrição de um arquivo de áudio para um arquivo de texto. Ainda levando em conta que a transcrição é fiel ao áudio na sua maior proporção, em alguns casos pode estar incompleta ou inexata por falta de fidelidade do áudio, bem como pode ter sido corrigida gramaticalmente para melhorar a qualidade e compreensão do texto. Esta transcrição é proporcionada como material adicional ao arquivo de áudio, mas não deve ser considerada como registro oficial.

MANAL ISMAIL:

Muito obrigado, Gulten, e sejam bem-vindos de volta, espero que tenham gostado das férias. Agora receberemos uma atualização de 30 minutos do Grupo de Trabalho de Segurança Pública do GAC, que fornecerá uma atualização sobre o trabalho do grupo de trabalho e seus objetivos estratégicos da sessão são de apenas 30 minutos, então, sem mais delongas, passarei diretamente para co-presidentes do Grupo de Trabalho de Segurança Pública Laureen Kapin e Christopher Lewis-Evans. Ambos os quais você já conheceu durante a sessão anterior. Teremos que terminar em perfeitas condições porque teremos o Conselho se juntando depois, então vou passar a palavra a você diretamente. Por favor. Quem vai começar?

LAUREEN KAPIN:

Eu vou. Obrigada, Manal. Portanto, estaremos muito atentos ao tempo, esta é uma agenda curta, revisaremos o trabalho de nosso Grupo de Trabalho de Segurança Pública, que tem estado muito ativo recentemente. Faremos um relatório sobre o progresso do plano de trabalho, todos esses materiais, a propósito, são para sua análise na parte do GAC do site da ICANN. Falaremos sobre nossa participação em vários fluxos de trabalho e, se o tempo permitir, retomaremos os tópicos da discussão sobre abusos de DNS que encerramos na apresentação sobre abusos de DNS. Próximo slide, por favor. Portanto, o Grupo de Trabalho de Segurança Pública tem objetivos bem definidos. Eles estão em nosso plano de trabalho e, de um modo geral, nos concentramos em questões que se concentram em proteger o público de práticas maliciosas ou enganosas e, a esse respeito, temos três componentes principais em nosso plano de trabalho: desenvolver

o abuso de DNS e o crime cibernético recursos de mitigação, e trabalhamos com nossos colegas, não apenas em todo o mundo na aplicação da lei e outras agências de segurança pública, mas também com nossos grupos de partes interessadas da comunidade, uma vez que podemos efetivamente fazer esse trabalho juntos ouvindo uns aos outros e garantindo que temos um sentido completo daqueles que estão mais bem posicionados para lidar com certas questões. O segundo grande grupo de atividades em que nos concentramos é o tópico principal de alguns de nossos trabalhos - trata dos serviços de diretório de registro de domínio que costumavam ser conhecidos como WHOIS. E afirmamos que a informação é uma ferramenta muito importante no cinto de ferramentas de aplicação da lei porque fornece informações sobre quem é responsável por um domínio, e isso entra em jogo se esse domínio estiver envolvido em atividades que podem ser ilegais enganosos. Portanto, é importante saber quem é o responsável por isso, e as informações de registro de domínio podem ajudar a esclarecer isso. E, finalmente, nosso outro objetivo é mais focado internamente e é garantir que um, tenhamos recursos suficientes para fazer o trabalho que estamos encarregados, e dois, que estamos alcançando a comunidade e grupos de partes interessadas e governos para certifique-se de que estamos atendendo às suas necessidades. E, se você quiser entrar em contato conosco sobre qualquer assunto, saiba que Chris e eu, e meus colegas do Grupo de Trabalho de Segurança Pública, estamos sempre disponíveis para ser contatados por e-mail, telefone ou qualquer dispositivo de comunicação que seja adequado ao que precisa. Estamos felizes em conversar. Chris, é com você.

CHRIS LEWIS-EVANS:

Sim, muito obrigado. Próximo slide, por favor. Então, eu só quero me aprofundar em nosso primeiro objetivo aqui, que é em torno do desenvolvimento de recursos de mitigação de abuso do primeiro que eu quero concentrar e são dois itens que agrupamos um pouco 1,2, 1,3 aqui e fizemos um progresso muito bom com os registros e registradores sobre medidas proativas e preventivas que eles podem tomar, e eu realmente queria chamar Gabriel Andrews, de quem ouvimos falar antes. Ele tem feito um trabalho muito bom com a casa das partes contratadas para lidar com botnets registrados por DGAs, que é um algoritmo de geração de domínio. Portanto, isso é muito importante para o trabalho que estamos fazendo. Também examinamos como os ccTLDs adotam alguns procedimentos e como isso pode ser transferido para o espaço de gTLDs. Acho que recebemos um bom feedback até agora dos ccTLDs, e agora precisamos apenas dedicar algum tempo trabalhando em como isso poderia ser transposto para o espaço dos gTLDs. Outro item que acho que já tocamos na sessão anterior é o último - e espero que no ICANN70, então amanhã acredito que vamos terminar este aqui e que trata dos impactos da criptografia DNS, principalmente DNS sobre HTTPS na mitigação de abusos de DNS. Obviamente, haverá mais desenvolvimentos, mas acho que fizemos a maior parte do trabalho nisso. Então, para mim, isso é apenas uma visão geral rápida na primeira tentativa. E, Laureen, com você para o segundo.

LAUREEN KAPIN:

É necessário ativar o som. Obrigada. Próximo slide. Portanto, nosso objetivo estratégico 2, como você se lembra, trata do acesso aos dados de registro de nomes de domínio. Você verá que nosso ótimo código de cores verde significa que está no caminho certo. O amarelo está em espera aguardando alguns desenvolvimentos e o vermelho significa que foi desafiado ou encontramos desafios que considero mais precisos. Então, apenas para destacar alguns desses itens, você verá que sinalizamos do GAC que estamos interessados em implementar rapidamente a fase um do EPD. Você sabe de nossa apresentação anterior que os cronogramas são um pouco incertos. Tivemos alguns bons desenvolvimentos nos mecanismos provisórios para acesso razoável, incluindo o fato de que o cumprimento do contrato agora tem um formulário dedicado para reclamações sobre o acesso aos dados WHOIS e também relatórios dessas reclamações. Portanto, esses são desenvolvimentos positivos. Você verá que observamos a necessidade de melhorar a precisão dos dados de registro e esperamos que esses esforços de desenvolvimento de políticas trabalhem com a contribuição do GAC para lidar com isso. Para que essa política funcione. Na Fase 2A, estamos nos concentrando nos esforços para correlacionar endereços de e-mail com outros registros de domínio para investigações de aplicação da lei. Essa é uma ferramenta muito poderosa que falta atualmente, e eu acho - 2.10 é o ponto final que discutirei aqui. Esta foi uma recomendação do CCT e você verá que ainda está na categoria vermelha. Basicamente, estamos recomendando, e eu digo nós, onde em meu membro anterior da equipe de revisão de CCT, estávamos recomendando que toda a cadeia de partes responsáveis por um domínio, incluindo revendedores, fosse

publicada no registro WHOIS e a razão pela qual isso é importante é que a aplicação da lei quando está buscando informações sobre um registrante, eles precisam saber a quem recorrer. E nem sempre é o registrador que pode ser o primeiro elo na cadeia que o registrador pode estar lidando com um revendedor que, na verdade, tem a relação contratual com o registrante. E pode ser mais de um revendedor. Portanto, é muito importante ter essas informações publicadas no registro DNS. Não é obrigatório agora e essa foi a recomendação da equipe de revisão do CCT, e - isso ainda é algo que está sob esforços de advocacy, direi. Esperamos que isso se torne um requisito e não apenas uma opção, que é o status quo.

CHRIS LEWIS-EVANS:

Obrigado, Laureen. Chris Lewis-Evans, para constar. O terceiro objetivo estratégico é manter o relacionamento com as partes interessadas e, obviamente, detalhar o plano de trabalho. Acho que o plano de trabalho foi bem documentado e o compartilhamos com nossos colegas do GAC várias vezes e, como sempre, você nos mantém honesto com esse plano de trabalho, e acho que fomos capazes de trabalhar muito bem com ele. Acho que lutamos um pouco, e acho que com todos os outros, com a situação do COVID-19, e você sabe que isso, acho que nos impactou ao sermos capazes de produzir alguns dos recursos de colaboração e compartilhá-los de forma eficaz, embora também entendendo a experiência, de todo o tipo de rede PSWG por falta de uma palavra melhor. Certamente, isso é algo que pretendemos expandir e acho que Laureen abordará isso no próximo slide. E no que diz respeito ao relacionamento com os outros stakeholders, temos

feito ações bilaterais com todos os demais stakeholders da comunidade, e estão indo muito bem. Tivemos um envolvimento muito bom com todas as partes interessadas que tivemos até agora e algumas conversas muito boas e interessantes nas quais esperamos realmente desenvolver alguns de nossos outros objetivos que destacamos. Laureen, de volta para você.

LAUREEN KAPIN:

Próximo slide, por favor. Portanto, como dizem no mundo dos infomerciais, este é o nosso apelo à ação. É aqui que estamos pedindo a vocês, nossos colegas do GAC, que considerem quem são os órgãos de segurança pública de proteção ao consumidor em sua jurisdição que podem estar interessados em participar do trabalho do Grupo de Trabalho de Segurança Pública? Na verdade, tivemos, tivemos 14 representantes se juntando ao Grupo de Trabalho de Segurança Pública desde ICANN69 e podemos ter ainda mais, e agradecemos sua contribuição para esses esforços. O PSWG é uma grande contribuição, como você pode. E na verdade - e eu acho - eu sempre escuto isso, mas na verdade é a arrecadação de fundos públicos para a estação de rádio aqui em Washington D.C. e suas técnicas de comunicação são muito relevantes. É, dê o que você puder. Se você não pode pagar uma pessoa inteira, tudo bem, porque ela pode realmente se concentrar em um tópico específico. Eles podem simplesmente enviá-lo por um caminho. Eles podem apenas participar de nossas ligações entre as sessões, que talvez durem cerca de uma vez por mês. Portanto, não estamos pedindo que alguém dedique horas e horas e semanas e semanas de esforço. É muito flexível e convidamos as pessoas a trazerem seus

conhecimentos e compartilhem suas perspectivas conosco, porque todos viemos de diferentes pontos de vista. Portanto, como eu disse, temos uma ou duas reuniões plenárias entre as sessões. Temos reuniões bilaterais informais com diferentes grupos de partes interessadas. Temos leads de tópico e, a propósito, não dizemos que você faça isso. Faça isso. Perguntamos às pessoas no que elas estão interessadas. E agora temos o que parece ser muitos membros e, de fato, são muitos membros, mas direi a vocês apenas entre nós, por assim dizer, o número de membros que temos não realmente não reflete o número de membros que participam ativamente do trabalho. E o que adoraríamos é ter mais membros que realmente estão interessados em participar do trabalho do dia-a-dia, então se você tiver dúvidas sobre isso, ou alguém que possa estar interessado, por favor, peça que entrem em contato com Chris ou eu, e teremos o maior prazer em apresentá-los às nossas atividades e informá-los sobre o que pode ser uma boa opção com base em seus próprios interesses. Neste momento, quero mudar e voltar a algumas de nossas discussões sobre abuso de DNS e, se eu pudesse perguntar - se eu pudesse pedir para ir para o slide 19, perfeito. E eu gostaria de falar primeiro em termos de abuso de DNS sobre o tópico que acompanha a apresentação de meu colega do Japão, que é a aplicação das cláusulas contratuais da ICANN e, na verdade, nosso contratado - nossas próprias partes contratadas apontaram para a aplicação das cláusulas contratuais da ICANN como uma das ferramentas principais e existentes que temos para combater o abuso de DNS e, é claro, estamos absolutamente de acordo em usar isso. E eu quero olhar para trás para alguns conselhos anteriores do GAC e posso ver que é do comunicado de Toronto e isso foi antes do

lançamento do novo gTLD, e o GAC havia avisado que se houver compromissos estabelecidos na solicitação de gTLD, esses devem ser transformados em contratos vinculativos, obrigações contratuais e estou enfatizando a vinculação mundial e, em seguida, no comunicado do GAC de Pequim, é claro, o GAC forneceu recomendações de salvaguardas muito específicas sobre o que deve ser aplicado a todos os novos gTLDs, um subconjunto especial de salvaguardas para GT e regulamentadas setores e ainda mais salvaguardas que se aplicariam a gTLDs altamente regulamentados, e esses são, por exemplo, os gTLDs que lidam com tópicos muito delicados. Os bancos, farmácias, contabilidade, certas organizações de saúde, instituições de caridade. Domínios onde você pode estar envolvido em transações muito confidenciais ou divulgando dados financeiros ou de saúde confidenciais. E foi isso que levou ao público ... compromissos estabelecidos nas especificações do contrato de registro 11. E na especificação 11, temos certas obrigações específicas, mas como foi apontado na discussão anterior que tivemos sobre as recomendações de SSR2, houve questões levantadas por Conformidade da ICANN, e de fato o board da ICANN, sobre o contrato do GAC. Então, apenas para aprofundar um pouco, a especificação 11 exige - isso é conhecido como um requisito downstream - que os registros exigem que os registradores incluam em seus contratos com registrantes - e é por isso que é downstream - vai desde o nível de registro ao nível de registrador para a pessoa que está comprando o domínio, o registrante - deve haver uma cláusula que basicamente diga para não fazer coisas ruins. Essa é minha paráfrase de alto nível, mas, mais especificamente, ela proíbe as pessoas que possuem os domínios. Os detentores de nomes

registrados, desde a distribuição de malware, botnets, phishing, pirataria, violação de marca registrada ou direitos autorais, práticas fraudulentas ou enganosas, falsificação ou qualquer outra forma de participação em instituições de caridade. Domínios onde você pode estar envolvido em transações muito confidenciais ou divulgando dados financeiros ou de saúde confidenciais. E foi isso que levou ao público ... compromissos estabelecidos nas especificações do contrato de registro 11. E na especificação 11, temos certas obrigações específicas, mas como foi apontado na discussão anterior que tivemos sobre as recomendações de SSR2, houve questões levantadas por Conformidade da ICANN, e de fato o board da ICANN, sobre o contrato do GAC. Então, apenas para aprofundar um pouco, a especificação 11 exige - isso é conhecido como um requisito downstream - que os registros exigem que os registradores incluam em seus contratos com registrantes - e é por isso que é downstream - vai desde o nível de registro ao nível de registrador para a pessoa que está comprando o domínio, o registrante - deve haver uma cláusula que basicamente diga para não fazer coisas ruins. Essa é minha paráfrase de alto nível, mas, mais especificamente, ela proíbe as pessoas que possuem os domínios. Os detentores de nomes registrados, desde a distribuição de malware, botnets, phishing, pirataria, violação de marca registrada ou direitos autorais, práticas fraudulentas ou enganosas, falsificação ou qualquer outra forma de participação em instituições de caridade. Domínios onde você pode estar envolvido em transações muito confidenciais ou divulgando dados financeiros ou de saúde confidenciais. E foi isso que levou aos compromissos públicos estabelecidos nas especificações do contrato de registro 11. E na especificação 11, temos certas obrigações

específicas, mas como foi apontado na discussão anterior que tivemos sobre as recomendações de SSR2, houve questões levantadas pela conformidade da ICANN, e, de fato, o board da ICANN, sobre o contrato do GAC. Então, apenas para aprofundar um pouco, a especificação 11 exige - isso é conhecido como um requisito downstream - que os registros exigem que os registradores incluam em seus contratos com registrantes - e é por isso que é downstream - vai desde o nível de registro ao nível de registrador para a pessoa que está comprando o domínio, o registrante - deve haver uma cláusula que basicamente diga para não fazer coisas ruins. Essa é minha paráfrase de alto nível, mas, mais especificamente, ela proíbe as pessoas que possuem os domínios. Os detentores de nomes registrados, desde a distribuição de malware, botnets, phishing, pirataria, violação de marca registrada ou direitos autorais, práticas fraudulentas ou enganosas, falsificação ou de outra forma se envolver na discussão na sessão de abuso de DNS, o próprio Conselho da ICANN levantou questões para as partes interessadas em propriedade intelectual grupo sobre fiscalização, e achei que valia a pena repetir porque você sabe que está entendendo da fonte aqui. As cláusulas do contrato como estão atualmente, e o motivo pelo qual estou discutindo isso é que acho que fornece um roteiro para a lacuna que podemos preencher - não pode - não concede à ICANN a aplicação ou direito contra registradores que não incluem o contrato exigido em seu contrato ou como determinar se os registradores impõem consequências para os proprietários de domínio que podem se envolver em atividades inadequadas. Então essa é uma lacuna. Além disso, em termos de contrato de registrador, ele não estabelece consequências específicas que os registradores devem impor se seus

registrantes se comportarem mal e, portanto, a aplicação da ICANN não tem autoridade para dizer aos registradores que excluam ou suspendam o domínio nomes ou para realizar certas ações específicas. Isso não é algo que está estabelecido no contrato, ou seja, não diz quais devem ser essas consequências. Diz apenas que deve haver consequências se eles se envolverem em comportamento ilícito.

E a conclusão aqui, eu acho, embora eu saiba que nossa equipe de revisão de procedimentos subsequentes não necessariamente concorda - mas em 2013 o novo contrato de gTLD forneceu uma oportunidade e continha salvaguardas mais específicas do que o contrato de gTLD anterior continha. Eles aumentaram o nível de proteção contra abusos de DNS, e certamente é uma oportunidade, se a próxima rodada ocorrer, defender que essa rodada poderia ter um desempenho ainda melhor em termos de cláusulas contratuais que são claras e exequíveis em relação às obrigações de mitigar abusos de DNS. E levo muito a sério que, em um mundo ideal, como declarou nossa equipe de revisão de procedimentos subsequente - lidaríamos com o abuso de DNS de forma holística, ou seja; em todos os gTLDs, mas, enquanto isso, acho que podemos lidar com isso de forma incremental, concentrando-nos em como as disposições do contrato podem ser melhoradas e se houver uma rodada subsequente para buscar a melhoria desses contratos como ponto de partida. Slide final em meus 3 minutos finais, chegando às definições de abuso de DNS que eu acho que é parte integrante, e eu toquei nisso no último, na última discussão. O que realmente quero que você descubra aqui é que não precisamos reinventar a roda. Aqui estou pegando emprestado o comentário APT

de alguém, não precisamos reinventar a roda sobre o abuso de DNS e muito desse trabalho já foi feito e isso é papel da equipe de revisão, dependendo do trabalho anterior feito por relatórios da ICANN equipe da organização. Também definições de consenso baseadas nos contratos. Novamente, esses já estão nos contratos. Eles já existem políticas e certamente podemos buscar essas fontes para chegar a um acordo sobre o que compreende o abuso de DNS e, por último, nosso colega Kavouss pediu para olhar um dos slides novamente, slide 16, eu queria colocar isso na tela para permitir que Kavouss acompanhe qualquer dúvida, e também, nos nossos últimos 2 minutos, se alguém tiver alguma dúvida, fico feliz em levá-la junto com meu colega.

IRÃ:

Desculpe voltar ao slide anterior. Se você olhar para as partes contratadas do terceiro ponto, o que você acha dessas reivindicações? É você que eles têm ferramentas limitadas e nem sempre adequadas e assim por diante. Então, não vou fazer um por um, mas o que podemos fazer sobre isso? Como poderíamos convencê-los? Como a situação poderia ser melhorada? Também tem a ver com o que você disse há 2 minutos que ir para as cláusulas dos contratos, ou cláusulas do contratado e melhorá-los, mas se quisermos melhorá-los e temos esse argumento de que eles mencionam que têm um limite e nem sempre o que podemos, podemos? Obrigada.

LAUREEN KAPIN:

É um desafio com certeza, Kavouss. Acho que, em primeiro lugar, não desprezo alguns de seus argumentos porque, em certos aspectos, eles

têm ferramentas limitadas e, às vezes, é um desafio para eles descobrir quem está melhor posicionado para lidar com o abuso, e eu dê o exemplo de quando há um conteúdo particularmente problemático em um domínio. Conteúdo que pode ser enganoso. Vou dar um exemplo de uma reclamação enganosa sobre o alívio COVID-19, alívio financeiro. Isso tem sido muito prevalente atualmente. E uma parte contratada pode dizer que não somos responsáveis por esse conteúdo que é o registrante ou o provedor de hospedagem da web e, nesse caso, acho que algo que realmente precisa ser explorado são os termos de serviço, quais termos de serviço - o registrador está com seu registrante e esses termos de serviço estão sendo cumpridos? E como isso se relaciona com as cláusulas contratuais atuais que criam uma responsabilidade entre o registrador e o registrante? Esse seria um exemplo em que precisamos entender a realidade do negócio, e também precisamos ter certeza de que os contratos existentes estão sendo cumpridos. Também gostaria de apontar alguns dos trabalhos existentes em andamento com esforços voluntários, que consideramos muito úteis, mas não substituam os requisitos, porque são os requisitos que entram em jogo quando você está lidando com problemas realmente ruins atores ou paraísos para abusos sistêmicos de DNS que, infelizmente, sabemos que ocorreram de vez em quando. Maná, sei que estamos um pouco atrasados, mas também sei que Steve tem uma dúvida. Eu devolvo para você.

STEVE CROCKER:

Muito obrigado. Seria muito difícil para as organizações de segurança pública obterem informações detalhadas de registro para domínios

que parecem estar envolvidos ou implicados em mau comportamento, exigir uma resposta explícita às solicitações de dados de registro. Concentrei-me apenas na obtenção da data para o início da investigação. Não o resto da aplicação.

LAUREEN KAPIN:

Eu sei que não é um desafio para todos. Não estou dizendo que toda vez que a aplicação da lei faz esse pedido, eles não entendem ou leva muito tempo, mas sei que tem havido desafios, especialmente ao lidar com provedores de proxy de privacidade que exigem processos formais que uma intimação ou um tribunal ordem e a resposta à sua segunda pergunta é, sim, isso seria muito, muito, muito útil.

STEVE CROCKER:

São três “muitos”.

MANAL ISMAIL:

Muito obrigado Steve, e há outra resposta do Gabriel também no chat se vocês quiserem ler, e com isso, permita-me agradecer a Laureen e ao Chris, muito obrigado para esta atualização informativa, isso conclui a atualização PSWG. Agora temos a segunda discussão sobre os procedimentos subsequentes e, por favor, a equipe de suporte me avise quando estivermos prontos para começar.

[FIM DA TRANSCRIÇÃO]