ICANN74 | Fórum de políticas – Discussões do GAC: Abusos do DNS
Terça-feira, 14 de junho de 2022 – 15h às 16h AMS

MANAL ISMAIL: Olá a todos. Vamos iniciar daqui a um minuto. Peço que tomem seus lugares.

Bem, estamos no prazo, bom dia, boa tarde e boa noite a todos. Na sala do GAC e no Zoom, bem-vindos de volta à sessão do GAC sobre abuso do DNS. Teremos 60 minutos, e a consideração das iniciativas da ICANN Org e do GAC, e seremos informados de novidades e das atividades do GAC no seu relacionamento com outras partes interessadas. Na tela, temos aqui no nosso painel, oradores do grupo de trabalho de segurança pública, Gabriel Andrews do FBI, Cathrin Bauer-Bulst, da comissão europeia, Laureen Kapin da comissão federal de comércio dos Estados Unidos, e Chris Lewis-Evans da agência nacional anticrime. Temos o representante do Japão no GAC que vai participar de forma remota. Teruyuki, muito obrigada, espero que não seja um horário muito ruim para você aí. O senhor Teruyuki é do ministério do interior e comunicações do Japão. Finalmente, teremos nosso orador convidado, Graeme Bunton, do instituto

de abuso de DNS. Então, sem mais delongas, passo a palavra aos panelistas. Chris, você vai começar.

CHRIS LEWIS-EVANS: Obrigado, e olá novamente a todos, Christopher Lewis-Evans e co-presidente do PSWG. O abuso de DNS é um tópico muito importante, outro sobre o qual estamos falando há algum tempo, temos uma agenda bastante cheia com alguns palestrantes muito bons, então não vou demorar muito para falar sobre os tópicos que vamos ir através. Vamos descrever por que isso é importante para nós novamente. Tem havido muita discussão sobre as tendências de abuso de DNS, então vamos cobrir alguns dos aspectos para isso, e então entregaremos ao nosso colega do Japão de uma apresentação de alguns abusos de DNS em seu país. Em seguida, veremos algumas perspectivas operacionais e iniciativas que estão em andamento levarão muito bem à apresentação de Graeme sobre a denúncia centralizada de abuso e, em seguida, veremos o papel da ICANN e da comunidade no combate ao abuso de DNS. Então, com isso, vou passar para Laureen. Obrigada.

LAUREEN KAPIN: Oi pessoal. Meu nome ainda é Laureen Kapin, mas desta vez estou falando na qualidade de uma das co-presidentes do Grupo de Trabalho de Segurança Pública, e estou tão feliz hoje que temos

todos os 3 co-presidentes na mesma reunião, na mesma mesa. É um mimo. Então, vamos começar com a questão de por que isso é importante, e se você está falando sobre por que algo é importante, às vezes você tem que começar com o quê, e o que provou ser um problema que tem muitas perspectivas diferentes, mas existem definições sobre o que constitui abuso do Sistema de Nomes de Domínio que o GAC incluiu em um recurso muito bom, se você ainda não olhou para ele e está interessado em aprender mais sobre esse tópico, o GAC colocou uma declaração que se concentrou especificamente no abuso de DNS e coletou muitas das definições de dentro da comunidade. Então, se você ainda não olhou para isso e está interessado nesta edição, recomendo que dê uma olhada. Mas algumas dessas definições incluem esse conceito de ameaças à segurança, e que se originou com o conselho de proteção de Pequim que acabou se tornando parte do contrato de registro básico para novos domínios genéricos de primeiro nível e essas ameaças à segurança incluíam phishing, malware e botnets. E também havia a equipe de revisão de concorrência e confiança do consumidor e parte de seu trabalho se concentrou em questões de confiança do consumidor, e eles apontaram para uma definição que definia o abuso de nomes de domínio como atividades coniventes ou não solicitadas intencionalmente enganosas que fazem uso ativo do DNS do domínio O sistema de nomes e/ou os procedimentos usados para registrar nomes de domínio e o relatório de revisão

do CCT também contêm algumas informações muito boas sobre o abuso de DNS e o histórico de trabalho na comunidade sobre esse assunto. Então, às vezes há um debate sobre os contornos da definição. Acho que o conceito-chave quando falamos dentro do ecossistema da ICANN é que qualquer trabalho feito precisa ser consistente com o Estatuto e os contornos definidos. Portanto, o GAC falou sobre isso em sua declaração sobre abuso de DNS e, a propósito, esses são links, então, se você for aos slides, poderá vincular as informações subjacentes com um clique de sua mão, mas essas ameaças constituem uma ameaça ao público, então são consumidores, pessoas que estão on-line, que seria você e eu, muitos de nós, e sua confiança no Sistema de Nomes de Domínio e também não são apenas as pessoas, é a infraestrutura. Uma ameaça à estabilidade de segurança e resiliência da infraestrutura do DNS e, novamente, essas palavras devem ser muito familiares porque estão consagradas nos Estatutos da ICANN. Eles são cruciais para o seu mandato. Então, parte do motivo pelo qual nós, mesmo de um Grupo de Trabalho de Segurança Pública, é reconhecer que o abuso do DNS e as ameaças à segurança pública significavam que havia um papel de defesa e um papel consultivo para o Comitê Consultivo Governamental que poderia ser construtivo, poderia ser útil, então em 2015, formamos formalmente o Grupo de Trabalho de Segurança Pública, e digo formalmente porque o pessoal de aplicação da lei e de proteção ao consumidor já estava

defendendo essas questões, mas essa foi uma forma de formar um grupo de trabalho específico dentro do GAC que poderia se concentrar nessas questões, principalmente, devido à sua importância. E não são apenas o GAC e o Grupo de Trabalho de Segurança Pública que estão preocupados com essas questões. Muitos, se não a maioria, dos grupos da comunidade de partes interessadas da ICANN priorizam a contenção do abuso de DNS e quero ter certeza de incluir nossos registradores e partes interessadas de registro nessa categoria, muitas pessoas na mesa, se não a maioria das pessoas na mesa entre os contratados com muita preocupação com sua reputação e com seus clientes e priorizar esse trabalho e seus esforços, incluindo seu esforço voluntário, têm sido muito importantes nessa área. Então, temos muita unanimidade em torno da ideia de que isso é um problema e que podemos fazer melhor. Na verdade, houve algumas discussões esta manhã no Grupo de Trabalho de Segurança Pública, onde ouvimos alguns de nossos colegas da ICANN que, você sabe, prontamente reconheceram que você sabe, os contratos que tratam dessas questões formam o piso, a base, dá como podemos esperar que as entidades respondam e lidem com o abuso de DNS, e esse piso pode ser aumentado e, em seguida, melhorias podem ser feitas. Portanto, o ponto é que há muito foco e atenção nessas questões e há muito trabalho bom a ser feito. A questão dos contratos em particular é importante porque essas são as regras do caminho no ecossistema da ICANN

sobre o que precisa acontecer, e houve um reconhecimento pela Diretoria da ICANN e pela conformidade da ICANN de que os contratos atuais podem ser melhorados, que eles não são suficientemente claros e não criam obrigações suficientemente executáveis sobre essa questão de abuso de DNS. E você verá isso nas discussões da comunidade e nas reuniões e declarações anteriores. Há uma correspondência muito específica da Diretoria em 12 de fevereiro de 2020, que reconhece explicitamente que existem algumas lacunas no contrato atual que criam desafios para a conformidade da ICANN, e isso também foi discutido em várias equipes de revisão, incluindo o consumidor e a confiança revise as pessoas das equipes de revisão de WHOIS e das equipes de revisão de segurança e estabilidade, e também dentro do grupo de trabalho do processo de desenvolvimento de políticas de procedimentos subsequentes de novos gTLDs. Todos esses acrônimos, então isso é uma espécie de visão geral de por que essa questão é importante, e também alguns reconhecimentos da comunidade sobre o trabalho que precisa ser feito, e muito reconhecimento por vários grupos de trabalho e equipes de revisão de que há coisas específicas que pode ser feito para tornar o Sistema de Nomes de Domínio mais seguro do que é atualmente em termos de abuso de DNS. Então com isso eu vou passar o bastão para Gabe, para Gabe. Sim.

GABRIEL ANDREWS: Oi, pessoal. Meu nome é Gabriel e quero pegar carona no pensamento de porque isso é importante para o GAC por um momento. Como o PSWG informou o GAC sobre algumas das formas mais prevalentes e prejudiciais de cibercrime que existem hoje, esquemas como ransomware ou esquema de comprometimento de e-mail comercial, muitas vezes dependem de phishing para primeiro colocar seus ganchos em suas vítimas. Para dizer de outra forma, os esforços que realizamos aqui para abordar categorias de abuso de DNS, como phishing ou disseminação de malware, ajudam a proteger todos os nossos cidadãos contra as formas mais prevalentes e prejudiciais de cibercrime atualmente. Algumas das ferramentas mais importantes para os funcionários de segurança pública, como a ferramenta WHOIS que usamos sempre que os registros de domínio precisam ser vinculados, são os registrantes. Essas ferramentas só existem porque a política da ICANN as criou e sustentou. Acredito que estamos prontos para o próximo slide. Tudo bem. Passando para algumas das atualizações de abuso de DNS sobre os relatórios de tendências que discutimos recentemente, como muitos do GAC já estão cientes, a organização da ICANN publicou e recentemente informou o GAC sobre um relatório que eles publicaram chamado último 4 anos em retrospectiva uma breve revisão das tendências de abuso de

DNS. Agora, este é um relatório no qual a ICANN tirou muitos domínios e a contagem desses domínios das chamadas listas de bloqueio de reputação. Estas são listas de domínios que foram observados fazendo coisas ruins. Que tipo de coisas ruins? Eles estavam olhando para SPAM, eles estavam olhando para phishing, eles estavam olhando para entrega de malware, eles estavam olhando para o comando e controle de botnets, redes de computadores comprometidos por bandidos. Eles contam esses domínios, e a ICANN procurou responder à pergunta, bem, se contarmos o número de domínios vistos em cada uma dessas categorias durante os últimos 4 anos, há alguma tendência observável que possamos ver? E tendo feito isso eles sentiram que sim que existem, de fato, e publicaram este relatório sobre isso. Lendo o relatório que fizemos com grande interesse porque ter um entendimento compartilhado dos fatos é fundamental para o progresso das conversas sobre abuso de DNS, percebemos que nos relatórios a conclusão óbvia foi que os domínios que eles contaram para SPAM excederam em muito os outros 3 categorias combinadas, o que foi interessante de ver, e obviamente tão bom quanto você pode ver que o SPAM está no vermelho abaixo da programação. Houve um declínio no número de domínios contabilizados para SPAM ao longo do tempo. Infelizmente, como o SPAM é tão volumoso, torna mais difícil para o olho humano discernir bem quais são as outras categorias e quais são as tendências lá e tentamos neste slide destacar na parte inferior

onde azul acredito ser phishing e amarelo são malwares. Pode ser difícil fazer uma boa provocação, existe uma tendência semelhante lá? Como foi observado no SPAM? Não acredito que possamos fazer uma determinação com base apenas nisso. Os autores da ICANN por trás do relatório se ofereceram para compartilhar os dados que foram usados para gerar conosco e, portanto, esperamos poder analisar essas tendências em potencial individualmente em suas categorias. De fato, o phishing segue essa mesma tendência de SPAM? A entrega de malware segue isso? E isso novamente é importante porque é usado, este é o comprometimento de e-mail que está na faixa de 20 bilhões de dólares de exposição a perdas globais a partir de 2019, 2020. Ransomware, novamente, usa phishing para comprometer as vítimas, então estes são perguntas muito importantes a serem respondidas e esperamos rever os dados no futuro. Além disso, e finalmente, observarei que os autores da ICANN neste relatório indicaram que tentariam determinar a causa dos altos e baixos dos domínios que estão contando para essas categorias de ameaças. Isso pode ser aguardado em um relatório futuro. Tudo isso para dizer que não estamos prontos para determinar que significado, se houver, deve ser extraído disso, mas esperamos mergulhar nele com mais detalhes em um futuro próximo. E obrigado.

LAUREEN KAPIN: Acho que nosso colega do Japão é o próximo, então talvez possamos passar para você e peço que avancem o slide para que possamos chegar à apresentação do nosso colega.

TERUYUKI SHIBATA: Posso falar?

MANAL ISMAIL: Sim, por favor, vá em frente.

TERUYUKI SHIBATA: Obrigado. Bom dia, boa tarde, boa noite, meu nome é Teruyuki Shibata, ministro das comunicações do Japão. Gostaria de expressar minha gratidão por ter recebido esta oportunidade de compartilhar com o Japão e também com vocês. Na reunião do ICANN72 e 73 do GAC, compartilhamos nossa opinião sobre as questões de salto de registradores e salto de domínio como exemplo de abuso de DNS. Hoje eu gostaria de apresentar algumas tendências recentes de abuso usando nomes de domínio e como violação de direitos autorais. Além disso, gostaria de compartilhar um caso usando nomes de domínio e popping mais, como você pode ver no diagrama à esquerda mais da metade das principais citações relacionadas a quadrinhos

japoneses, um domínio quente, de fevereiro a abril de 2022. Alguns sites importantes foram fechados. Em seguida, como você pode ver no diálogo do lado direito, o abuso de nomes de domínio tende a se concentrar em alguns registradores específicos. Concentrado em registros especificados. Algumas semanas atrás, eles tiveram uma reunião com uma área que um nome de domínio que tinha registrador sendo abusado, então temos que realizar nossa primeira discussão sobre esse assunto. Portanto, gostaríamos de propor algumas sugestões sobre como essas questões podem ser abordadas para evitar o abuso de nomes de domínio e registradores. A primeira é garantir a conformidade entre a ICANN e os registradores. De acordo com RA, um ex-registrador deve coletar informações de registrantes, como nomes, números de telefone e endereço postal. Como uma ação para selecionar essas informações, os registradores também devem considerar a verificação da camada 3 dessas informações coletadas. Por exemplo, eu sei entre registrador e registrantes que registrador verificamos as informações dos registrantes. Como uma ação de médio a longo prazo, gostaríamos de sugerir a adição de registradores dessas informações coletadas de registrantes. Em seguida, gostaríamos de sugerir a apreciação da disposição de que os registradores devem tomar medidas para incorporar, investigar a causa do abuso. Além disso, também gostaríamos de propor a conformidade da ICANN nesta auditoria. Acreditamos que é

importante continuar pensando no que a ICANN pode fazer e implementar para melhorar o ambiente da Internet. Espero ver progresso na discussão sobre esse assunto nesta reunião do GAC. Próxima página, por favor. Em seguida, gostaríamos de compartilhar o conceito de fluxo livre de dados com confiança. O conceito foi, na reunião de 2019 e na reunião do G20 em Osaka. O fluxo livre de dados deve aproveitar as oportunidades com treliça. Fortalecimento da treliça pelo enfrentamento contínuo dos desafios relacionados à privacidade. Proteção de dados. Os direitos de propriedade intelectual, irão facilitar o livre fluxo de dados em relação a esta sessão, é precisamente esta chave, confiança que se baseia neste conceito que gostaríamos de partilhar 3 pontos que devem ser apontados. Em primeiro lugar, a liberdade de expressão e o livre fluxo de informações devem ser protegidos. A segunda informação precisa garantir, a terceira Internet segura deve ser protegida. Esperamos que este conceito funcione. Muito obrigado, muito obrigado pela atenção. Obrigada.

CHRIS LEWIS-EVANS: Muito obrigado. Apresentação interessante. No próximo slide, abordaremos algumas perspectivas operacionais e iniciativas dentro da comunidade. Assim, a Comissão Europeia deu-nos a oportunidade de nos encontrarmos com alguns colegas responsáveis pela aplicação da lei e com a Europol.

Considerando a proximidade com a Europol, foi útil e tivemos algumas boas discussões sobre o abuso de DNS e os desafios que as agências de aplicação da lei enfrentam para lidar com isso. E um dos itens lá, não é necessariamente apenas interromper as entidades criminosas que causam o abuso de DNS, mas também identificar e proteger vítimas de crimes cibernéticos, fraudes, qualquer coisa que seja realizada utilizando a Internet e quebrar essa confiança na Internet. Em seguida, avançamos e conversamos sobre as tendências. Um dos pontos levantados na reunião é que a redução no número de domínios não dá uma visão holística do que está acontecendo no tipo de estrutura de abuso de DNS, ou visão geral, e realmente precisamos dar uma olhada nos danos que estão sendo causado; o número de vítimas, o número de denúncias de crimes cibernéticos. Essas são todas as informações que a ICANN obviamente não consegue obter por meio de seus métodos normais de coleta, e algo realmente que o PSWG e os membros da lei podem ter acesso. Então, a partir disso, veremos como podemos adicionar algumas das estatísticas sobre o abuso de DNS para ver a eficácia de algumas das medidas que estão sendo tomadas realmente impactam o abuso de DNS e contribuem para a redução do abuso de DNS. Portanto, como copresidentes do PSWG, se você tiver estatísticas ou relatórios realmente bons em agências que coletam esses dados, ficaremos muito felizes em ouvi-lo. A Europol ofereceu-se para fazer algum trabalho sobre este assunto e também irei

recolher alguns de outros países. E estamos ansiosos para apresentar isso em nossa próxima ICANN. Então, passando para as iniciativas atuais e futuras, uma das iniciativas da ICANN que foi concluída recentemente e eu sempre luto com a sigla, então direi na íntegra é o grupo de estudo técnico da iniciativa de facilitação de segurança de abuso de DNS, ou DSFI-TSG, eu entendi pela primeira vez naquela época, uma das regiões dentro de lá era a recomendação 5 que apontava para uma plataforma de compartilhamento de informações, isso é algo como grupos de segurança pública com os quais estamos bastante acostumados a lidar, há alguns exemplos muito bons certamente no espécie de instituições financeiras. Eles têm centros de compartilhamento e avaliação de informações muito fortes, e isso permite que esses institutos compartilhem informações sobre ameaças que estão vendo, tendências diferentes, maneiras de combater o abuso que estão vendo e fornecer as melhores práticas. Realmente vemos essa recomendação como um bom passo à frente na criação de tal plataforma, dentro da ICANN e das partes contratadas e para que outros grupos se juntem para ajudar a combater o abuso de DNS, e realmente veríamos isso como uma das principais recomendações desse relatório do grupo de estudo técnico para levar adiante e ser priorizado. Graeme vai falar sobre outro, então não vou estragar muito a apresentação dele, mas vou entrar nisso, mas há alguns outros frameworks voluntários muito bons que foram realizados. Com

isso, tudo isso tem um impacto realmente positivo em nossa capacidade de combater o abuso de DNS, no entanto, tem algumas limitações. Este não é o de Graeme, apenas geralmente, o voluntário apenas para ajudá-lo lá Graeme, pois eles não se aplicam necessariamente a todas as partes contratadas, então ainda vemos a necessidade de cláusulas contratuais aprimoradas ou mais trabalho de política para fazer isso se aplica a todas as partes contratadas e para poder combater o abuso de DNS de forma eficaz. E então com isso, Graeme, eu passo para você.

MANAL ISMAIL: Sim, por favor, vá em frente, Kavouss.

IRÃ: Sim, obrigado. Senhora, em primeiro lugar, gostaria de agradecer imensamente à ICANN pelo relatório sobre este assunto tão importante. Acho muito apreciado todos os esforços que foram feitos, todos os detalhes foram fornecidos número 1. Número 2, senhora presidente, pedimos a gentileza de levar este relatório com cuidado em nossas ações futuras, em particular com relação a qualquer conselho futuro ou acompanhamento o conselho do GAC relacionado ao abuso porque acho que este relatório forneceu ou atende a algumas dessas preocupações e não gostaríamos de repetir o que dissemos, agora temos alguma

resposta, talvez não respondendo totalmente ao que estamos pensando, mas acho que pelo menos na maior medida é satisfatório, então vou pedir a gentileza de seguir esse conselho quando redigirmos o Comunicado, ou acompanhar a ação do Comunicado anterior, levamos isso em consideração. Muito obrigado por isso.

MANAL ISMAIL: Muito obrigado Kavouss. Anotado, e também gostaria de chamar a atenção de todos para o bate-papo, então, por favor, fique de olho no bate-papo e vejo uma mão da Indonésia. Ashwin, por favor, vá em frente.

INDONÉSIA: Obrigado. Sua segurança, como abuso de DNS e assim por diante, é muito importante hoje, bem, não apenas hoje, mas há muitos anos, mas talvez hoje seja mais importante porque agora somos cada vez mais dependentes e a Internet por causa desse problema ruim do COVID-19, você vê.

IRÃ: Não devemos converter seu comitê em um grupo de redação. Obrigado.

MANAL ISMAIL: Obrigado, Kavouss. Desculpe, Ashwin, por favor, vá em frente.

INDONÉSIA: O que quero dizer é que talvez uma melhor cooperação possa produzir uma melhor segurança cibernética porque a TI, por exemplo, também propõe uma agenda de segurança global, por exemplo, como incluir a segurança cibernética há muitos anos e foi discutido durante o WCIT em Dubai, 2012 em Dubai, como a governança da Internet pode ser aprimorada pode ser para que a segurança cibernética esteja se tornando melhor. Naquela época, em Dubai, falamos mais sobre isso, então talvez à luz de mais segurança cibernética, esse tipo de operação pode ser rediscutida novamente, isso é tudo. Obrigada.

MANAL ISMAIL: Muito obrigado, Ashwin. E vejo uma mão dos EUA também, então, por favor, Susan vá em frente.

ESTADOS UNIDOS: Obrigado, presidente, e quero agradecer aos copresidentes do Grupo de Trabalho de Segurança Pública pela apresentação muito abrangente e maravilhosa que você acabou de fazer. Acreditamos que as soluções para lidar com o abuso de DNS podem assumir a forma de requisitos de contrato aprimorados, e Chris destacou que as iniciativas voluntárias são diferentes dos

requisitos de contrato e programas de conformidade que se aplicam a todos os registradores, e também acreditamos que as soluções podem incluir incentivos para alcançar métricas anti-abuso relevantes e processos de desenvolvimento de políticas também. Eu queria observar que nas discussões da perspectiva dos EUA e nas discussões sobre o abuso de DNS, parece que havia uma equação de igualar o abuso de DNS a qualquer coisa que seria prejudicial na Internet, é algo que eu vi, mas penso a transcrição, mas prejudicial em uma atividade legal na camada de conteúdo da Internet está fora do mandato da ICANN e, embora acreditemos, deva ser tratada com urgência, seja por meio de processo legal normal ou outras soluções voluntárias e colaborativas entre comunidades, como notificadores confiáveis e iniciativas de melhores práticas. Obrigada.

MANAL ISMAIL: Muito obrigado, US, e vejo uma mão levantada também, por favor, vá em frente.

PAÍSES BAIXOS: Obrigado, senhora cadeira. Boa tarde, colegas. Gostaria de abordar o comentário do nosso comentário indonésio sobre o uso da agenda global de segurança cibernética. Embora eu diga que é bom olhar para a cooperação com outras organizações, sinto que devemos encontrar uma solução aqui em casa como

parte do modelo multissetorial e não olhar muito, especialmente para os critérios que tínhamos em 2012, sabendo onde eles terminaram, e também levar em consideração que é há dez anos e acho que o mundo mudou e um pouco a partir daí.

MANAL ISMAIL: Muito obrigado, e não vendo mais pedidos para a palavra de volta, Graeme, e desculpe interromper seu início.

GRAEME BUNTON: Obrigado, Manal, e obrigado por me receber aqui hoje. Estou animado para falar com você sobre o lançamento do NetBeacon. Eu tenho um monte de slides para passar, mas o que é realmente claro é que o DNS Abuse Institute, com o apoio do PIR e lançamento limpo do DNS, adiciona o serviço de relatório de abuso de DNS centralizado disponível agora para simplificar o processo de denúncia de abuso de DNS e para fornecer valor para registrar estressores e registradores e torná-los mais fáceis de agir em casos de abuso. E mais substância por trás disso, o DNS Abuse Institute foi criado no ano passado pelo registro de interesse público que opera o TLD.org e a missão sem fins lucrativos de serviço e eles viram, como eu fiz quando entrei, que o abuso de DNS é um problema global complicado, e que a mitigação no registro e registradores individuais é seguida, e um trabalho centralizado coordenado é necessário para corrigir esse

problema e reduzir o abuso de DNS. E essa é a razão pela qual o instituto do abuso existe, é combater esse problema para induzir o abuso de DNS e fazê-lo de uma maneira que possamos coordenar em todo o DNS. Próximo slide, por favor. Assim, o NetBeacon, o serviço centralizado de denúncia de abuso, responde diretamente a vários esforços da comunidade e, portanto, a recomendação 13.1 do SSR2 exige um abuso de DNS central, no SSAC 115 falou sobre um relatório de abuso centralizado e o relatório CCRT aludiu a algo como um projeto como este. E assim nós olhamos como estávamos o instituto estava olhando para os problemas que poderia tentar e resolver parecia um lugar onde poderíamos fazer a diferença. Próximo slide, por favor. Certo. Portanto, existem 2 problemas fundamentais na denúncia de abuso hoje, ou havia. Denunciar abuso é difícil para aqueles de como fizeram isso. Talvez você tenha trabalhado para a comunidade de aplicação da lei ou a comunidade de segurança cibernética, é muito difícil fazer isso em todo o ecossistema e, para os usuários finais, é especialmente difícil. Exige conhecimento técnico. Você precisa ser capaz de identificar um registrador, você precisa encontrar sua página de denúncia de abuso, não há padrões consistentes reais para evidências, implementação dessas funções de denúncia de abuso e, portanto, é realmente bastante complicado. E o outro lado, e nem sempre apreciado, é que os relatórios de abuso que os registros e registradores recebem são, em geral, horríveis. Eles

não são estruturados, não são comprovados, geralmente são para domínios que não pertencem ao provedor, frequentemente não acionáveis e, portanto, os registros e registradores gastam muito tempo triando tickets por muito pouco valor de uma maneira que não torna a Internet nenhuma mais seguro. E então realmente sentimos que havia uma solução para isso que poderia ficar no meio e resolver os dois problemas de uma vez e isso é o NetBeacon. Próximo slide, por favor. Portanto, é uma ferramenta gratuita. É grátis para as pessoas enviarem e grátis para registros e registre-se começar a interagir com que aceita denúncias de abuso de DNS para phishing, malware, botnets e SPAM. Ele pega esses relatórios de abuso e os padroniza. Ele padroniza os requisitos de evidência e o formato, enriquece esses relatórios, de modo que não apenas pegamos o que foi enviado pelo usuário final, mas também pegamos esse nome de domínio ou URL e o comparamos com várias fontes on-line de inteligência de domínio. Podemos descobrir mais alguma coisa sobre este domínio? Existem outros hits por estar envolvido em atividades ilegais ou atividades ruins? E, em seguida, anexar isso ao relatório de abuso e isso é importante porque é aqui que encontramos incentivo para usar esse serviço de registros e registradores, porque agora o que eles estão recebendo é mais informações, e mudamos até certo ponto alguns desses serviços investigativos carga da pessoa de compliance da linha de frente para o próprio serviço. E o que estamos tentando fazer é reduzir a barreira de

ação no registro ou registrador para que eles possam obter um relatório de abuso robusto, completo e padronizado, em que tudo o que eles precisam fazer nesse momento é escolher se é prejudicial e como responder. Outra característica importante é que estamos distribuindo-os automaticamente. Nós removemos o fardo do repórter entender onde isso precisa ir. Estamos fazendo isso por eles. Próximo slide, por favor. Portanto, isso é importante para entender a escala do problema que estamos perseguindo aqui. Você sabe um pouco de todos os abusos de DNS na Internet. Parte disso é descoberto em listas e feeds. Esta é a lista de bloqueio de reputação da RBL que é a espinha dorsal de muito trabalho de segurança e mede o abuso de DNS, mas também há esse outro subconjunto de abuso relatado manualmente e é realmente isso que consome muito registro e início de ciclos de abuso de registro de suas horas e é isso que eles estão gastando muito tempo fazendo triagem por muito pouco valor e, portanto, esse é realmente o problema que estamos tentando atingir com o NetBeacon. Próximo slide, por favor. Este é um exemplo do relatório de phishing. Então, se você for para o NetBeacon ou precisa se inscrever em app.NetBeacon.org, onde você pode ir e criar um relatório de abuso de phishing. É fácil de usar muito os campos são diretos. Tentamos fornecer dicas úteis de ferramentas explicando quais informações são necessárias. Eu acho que a interface do usuário é muito boa. E relativamente simples para a maioria dos usuários se envolverem. Vou notar

que há um pouco de atrito aqui. Algumas pessoas não querem que usemos formulários, mas infelizmente, o texto livre é simplesmente impraticável na escala da Internet. Registros e registradores exigem uma ação mais estruturada para agir com eficácia um do outro, caso exigimos um endereço de e-mail funcional. Você precisa ser capaz de verificar seu e-mail para enviar denúncias de abuso porque somos apenas um intermediário. Estamos fazendo essas denúncias de abuso, tornando-as melhores e padronizadas, mas levá-las até onde eu preciso para a GNSO e um registro ou registrador requer mais informações de que precisam para poder entrar em contato com a pessoa que as enviou. Portanto, não há denúncia anônima de abuso por meio deste serviço. Próximo slide, por favor. Alguns outros recursos rápidos. Há uma API para envio de relatórios para que a segurança cibernética, a aplicação da lei, os usuários finais que podem denunciar abusos em escala possam ser habilitados a fazê-lo. Nós não ativamos isso. Temos que descobrir as regras e a quantidade de trabalho para fazer isso e precisamos garantir que a qualidade dos relatórios de abuso seja realmente alta para que os registradores vejam o valor da ferramenta, mas vamos permitir isso em um futuro próximo. Há também uma API para relatar o consumo aos registros e os registradores podem consumir os relatórios não apenas por e-mail. Assim, eles podem inseri-los nos sistemas de gerenciamento de abuso e esses formulários são incorporáveis para que os registradores e

registradores qualquer outra pessoa possa incorporá-los nos sites, permitir a denúncia de abuso, obter o valor da padronização e enriquecer sem fazer o trabalho de desenvolvimento por conta própria. Próximo slide, por favor. Isso é importante porque quero ter certeza de que cobrimos o que é e o que não é. Não é gestão de abuso. Cadastros e registradores os receberão no sistema onde se sentirem confortáveis. Não é um lugar onde eles vão gerenciar suas queixas de abuso. Também não faz determinações. Sempre caberá ao registro ou registrador que tem a responsabilidade de determinar, em última análise, se isso é abuso e como responder a isso. Também não estamos construindo um repositório de reclamações de abuso. É um risco para o instituto, e também os registros e registradores não ficariam felizes se estivéssemos armazenando suas roupas sujas para sempre, por isso temos uma política de retenção de dados relativamente curta. E não se trata de fornecer acesso às informações do registrante. Os registradores já têm isso. Eles geralmente não precisam disso para enviar abuso de dados. Trata-se realmente de interromper o abuso. Não se trata de tentar ter um longo vai-e-vem ou obter acesso à informação. Próximo slide, por favor. Temos uma agenda bastante ambiciosa para este serviço. Nós realmente queremos construir uma nova ferramenta central robusta que seja um bem público para tornar a Internet mais segura. Isso inclui a integração de ccTLDs que hospedam redes de distribuição de conteúdo e provedores de

serviços de e-mail para que possamos aceitar relatórios de uma ampla gama de danos e encaminhá-los para onde eles pertencem. Isso nos permite fazer coisas como ter caminhos de escalonamento para que o abuso possa ser relatado às empresas de hospedagem e, em seguida, podemos encaminhá-los para o registrador, quando apropriado. O melhor exemplo seria para sites comprometidos onde alguém foi invadido sem saber e agir primeiro na camada DNS é muitas vezes inadequado, então podemos enviar isso para o host ET primeiro, você sabe que podemos ver se eles tomam medidas e escalam ainda mais. Em última análise, queremos também obter a reputação do denunciante, para que as pessoas que denunciam abusos e fazem isso comercialmente e desejam demonstrar uma reputação de serem muito bons em denunciar abusos possam ter um terceiro neutro no NetBeacon para demonstrar que são bons em este. Ao mesmo tempo, os registros e registradores querem alguma garantia às pessoas de quem estão recebendo denúncias de abuso, ou o fazem de boa fé e o fazem com qualidade robusta, e estamos trabalhando para isso também. Próximo slide, por favor. Algumas perguntas frequentes. É fácil para os usuários finais? Acho bem fácil. Provavelmente não precisamos fazer nenhum trabalho de UX e pensar um pouco mais sobre isso, mas em geral quase todo mundo poderia usá-lo agora. Atualmente, é apenas em inglês. Precisamos continuar limpando o texto, mas no final das contas estaremos traduzindo isso para disponibilizá-

lo em todo o mundo. Muitas vezes recebo perguntas sobre se publicaremos os dados que estão passando por isso. Assim como os relatórios, a resposta curta é que provavelmente produziremos algumas estatísticas agregadas, mas achamos que a adoção dessa ferramenta é mais importante do que envergonhar os registradores que têm relatórios de abuso que passam por ela. O DNS SI tem uma iniciativa separada para medir o abuso de DNS que eu acho que será academicamente rigorosa e muito mais robusta em resposta a essa pergunta específica. Encerramento e notificações. Não podemos fechar tíquetes para registradores que sempre dependerão deles. Acho que há um trabalho interessante a ser feito em torno do gerenciamento de expectativas dentro desta comunidade e espero que isso se torne uma peça de discussão. Outra pergunta frequente que devo acrescentar é se os registradores precisam se inscrever e a resposta é não. Os registradores são obrigados a ter um contato público de denúncia de abuso e é para isso que estamos enviando por padrão. Registradores e obtêm valor criando uma conta, mas não precisamos deles para fazer isso. Próximo slide, por favor. Este surge, bem como um FAQ mais geral. Por que estamos fazendo isso? E acho que isso é importante na resposta quando você está analisando o abuso e como denunciá-lo pela Internet muito rapidamente, torna-se evidente que fazê-lo de forma eficaz exige trabalhar mais do que apenas registros e registradores. Você precisa se envolver com outras partes da infraestrutura da

Internet e fazer isso muito rapidamente cruza a competência da ICANN. Então, nós realmente nos sentimos como um membro ágil e respeitado desta comunidade, bem apoiado, estaríamos bem posicionados para construir um serviço como este. E há outro artigo aqui sobre registradores de registros e empresas de hospedagem que têm vários locais para denunciar abusos, e eles acabam sabendo que se houvesse apenas uma iniciativa da ICANN, você acaba bifurcando seus processos de denúncia de abuso e isso não funciona. Isso cria confusão para usuários finais e pessoas que tentam denunciar abusos. Próximo slide, por favor. Certo, apoiando o trabalho. Então, algumas das definições iniciais deste projeto em que trabalhamos com o projeto de Internet e jurisdição, então obrigado a eles. E então o PPIR é um apoiador do DNS Abuse Institute e este trabalho e DNS limpo apressam um parceiro extremamente generoso e doou a tecnologia, bem como as horas de desenvolvimento para personalizá-lo para nossos propósitos, então um grande obrigado a todos eles. Próximo slide, por favor. Então isso é ao vivo. Qualquer um pode ir visitá-lo. Você pode criar uma conta se tiver abuso para denunciar. Por favor, faça isso. Você pode entrar em contato diretamente comigo para obter mais informações. E então estou sempre interessado em fazer conexões com organizações que desejam interromper o abuso de DNS e podemos conversar sobre como integrar com a ferramenta.

Então é isso. Espero que haja perguntas. Fico feliz em responder a qualquer que tenhamos. Muito obrigado pelo tempo.

MANAL ISMAIL: Já posso ver uma mão levantada. Então, na sala do Zoom, por favor, desculpe se estou pronunciando errado e então tenho Nigel Hickson do Reino Unido, por favor.

NÃO IDENTIFICADO: É possível que os proprietários de domínio recebam relatórios do NetBeacon? Somos um domínio e seria útil para nós sabermos que os domínios abusivos estavam sendo registrados que eram semelhantes a nós ou meio que se passavam por nós, então seria possível obter um feed do que está sendo relatado relacionado ao nosso específico domínio.

GRAEME BUNTON: Obrigado pela pergunta. É interessante, e não pensei muito sobre isso, então certamente não construímos muito a semelhança é um problema interessante. Acho que teríamos que ter algo relativamente sofisticado para fazer isso, mas vou adicionar à lista de recursos porque há muito trabalho a ser feito e vamos dar uma olhada nisso, obrigado.

REINO UNIDO: Sim, muito obrigado e muito obrigado, Graeme, por isso. Bem, obrigado por todo o painel, foi excelente. Mas em particular Graeme pelo incrível trabalho que você está fazendo no DNS Institute e neste NetBeason.

MANAL ISMAIL: Kavouss, temos uma intervenção aqui. Você está interrompendo uma intervenção, então, por favor, espere até que Nigel termine e eu vou lhe dar a palavra em seguida. Obrigada. Desculpe, Nigel. Por favor, vá em frente.

REINO UNIDO: De jeito nenhum. Boa tarde, Kavous. Perdi meu tópico, mas queria agradecer pelo que você sabe, pelo que está fazendo no NetBeacon. Isso soa incrivelmente positivo e eu realmente quero dizer isso porque acho que você sabe que ter essa riqueza de informações é realmente positivo. E suponho que a pergunta, a pergunta que eu tinha, e sei que você abordou parcialmente isso, mas você sabe, você trabalhou muito em termos de análise das informações relatando de volta ao registrador, fornecendo muitas informações diferentes, e, claro, no final das contas, tem que ser a determinação deles o que eles fazem com essa informação, mas acho que você está intrigado e nós ficaríamos intrigados como governos, suponho que você saiba, que um resultado positivo aconteceu, e eu sei que positivo é uma palavra

um pouco subjetiva, mas você sabe onde realmente houve abuso que esse domínio foi retirado ou qualquer outra coisa. Mas de qualquer forma, obrigado.

GRAEME BUNTON: Obrigado, Nigel. Eu aprecio essas palavras gentis. Estamos analisando como medir o resultado das denúncias de abuso, acho que é relativamente complicado fazer isso e é difícil dizer. Pode ser que você saiba que o relatório estava errado ou incorreto e, na verdade, deixar um domínio ativo era a coisa certa a fazer, mas estamos investigando isso e, em parte, por razões egoístas, queremos mostrar que o serviço está funcionando e tornando a Internet mais segura e então isso está na nossa lista de coisas para tentar e olhar.

MANAL ISMAIL: Muito obrigado. Então eu tenho Kavouss, então tenho Ruanda e então acho que precisamos prosseguir porque podemos estar ficando sem tempo. Então Kavouss, por favor, venha até você e me ajude a fazer um trabalho melhor, por favor, se você puder levantar a mão para que eu possa conhecer a fila, me desculpe. Vá em frente Kavouss. Kavouss você pode me ouvir? Então Ruanda, por favor, vá em frente.

RUANDA: Obrigado pelo DNS Abuse Institute, está bem feito e agradecemos. E eu só quero perguntar se você tem alguma qualificação, que você pode ajudar os países em desenvolvimento no abuso de DNS, e como você sabe, muitos países não têm os meios, e eu me comprometo a fazer uma cooperação com o domínio do código do país e engenheiros para poder evitar o abuso de DNS para ajudar a aumentar a segurança do domínio, e o último, eu só quero saber a frequência de publicação do seu relatório. Não sei se é um relatório anual ou apenas como você publica seu relatório. Obrigada.

GRAEME BUNTON: Obrigado por essa pergunta. No que diz respeito à capacitação, algumas das outras atividades em que o DNS Abuse Institute está envolvido são relacionadas à educação e práticas recomendadas, publicamos algumas delas para registros e registradores, bem como para usuários finais, para manter seus sites mais seguros e protegidos e reduzindo o abuso de DNS dessa forma. E esse é um trabalho que continuaremos a fazer como instituto ao longo do tempo. E, ansiosos para se envolver com você sobre isso. Obrigada. Ah, e relatório, não está claro que tipo de relatório vamos publicar no NetBeacon, mas como publicamos em um projeto separado medindo o abuso de DNS,

espero que comece a sair em agosto ou setembro e faremos isso mensalmente.

MANAL ISMAIL: Muito obrigado. Vejo uma mão dos EUA e me pergunto quantos slides temos? 2 slides? Então, EUA muito brevemente, porque precisamos seguir em frente. Vá em frente.

ESTADOS UNIDOS: Obrigado, presidente, e obrigado a Graeme pela apresentação. Os EUA reconhecem a introdução da ferramenta de relatório de abuso NetBeacon para iniciativas de abuso de DNS e também observamos sua consistência com as regiões feitas no relatório final do sack 115 e do SSR2 e esperamos conhecer mais desenvolvimentos sobre o uso e a implantação do NetBeacon antes do ICANN75. De maneira mais geral, sobre os relatórios de abuso de DNS, os EUA acreditam que uma atividade de relatório mais abrangente e rigorosa para incluir relatórios de abuso pode ser granular ao nível de registrador e registro. no desenvolvimento das cláusulas contratuais mencionadas anteriormente na apresentação. Obrigada.

GRAEME BUNTON: Obrigado por essas palavras tão gentis e eu provavelmente deveria mencionar que o serviço está ao vivo e está funcionando.

Tivemos o primeiro fluxo real de denúncias de abuso devido a isso e domínios ruins estão saindo da Internet e acho que é uma iniciativa realmente positiva olhando para o futuro. Obrigada.

MANAL ISMAIL: Muito obrigado, Graeme. E Cathrin, muito obrigado por sua paciência. Por favor, vá em frente.

COMISSÃO EUROPEIA: Sim, e obrigado da nossa parte. Passamos de horrível para ótimo, gratuito e fácil de usar. Realmente um avanço. E, para constar, sou Cathrin Bauer- Bulst. Estou com a Comissão Europeia e absolutamente emocionado em ver tantos de vocês de novo pessoalmente depois de uma pausa tão longa. Olá, seguidores do GAC. Então, vamos completar isso e voltar ao papel da ICANN. Qual é o papel da ICANN nisso? E o que deveria ser? Agora fizemos grandes progressos na criação de paciência do STRANS em relação ao abuso. Não apenas fora da ICANN. A própria ICANN contribuiu por meio da iniciativa DARR e do adesivo DNS e aqui estamos dando grandes passos quando se trata de utilizar tecnologia e automação para ajudar todo o ecossistema a ser mais eficiente no combate ao abuso. Vamos fechar o círculo para as primeiras observações de Laureen sobre a palavra. Hoje, a ICANN tem meios fáceis de agir quando um registrador não paga suas cotas. Mas não se o registrador violar repetidamente sua

responsabilidade de contribuir para uma Internet mais segura e resiliente, agora esse status quo não reflete totalmente a missão da ICANN e ouvimos muitos ecos dessa visão na comunidade. Existe um amplo consenso de que precisamos fazer mais e agradecemos o apoio do setor para várias iniciativas valiosas que já estão em andamento na ICANN e além. Agora, precisamos construir por um lado a transparência que agora está sendo criada. O compartilhamento de informações já citado pode desempenhar um papel fundamental. Precisamos construir isso e entender melhor os fatores que impulsionam o abuso de DNS em suas formas e apoiar as indústrias recreativas e registradores e complementar os dados da perspectiva da segurança cibernética com o que as autoridades de segurança pública e outros veem em suas investigações sobre a economia e também sobre o impacto humano de várias formas de abuso de DNS. E acreditamos que isso está precisamente de acordo com o papel da ICANN, conforme definido no contrato social e no Estatuto, conforme estabelecido como lembrete aqui. Agora, é claro que podemos criar transparência e facilitar tudo o que queremos. Também precisamos de incentivos. Porque, no final das contas, tomar medidas contra o abuso de DNS é um ponto de custo, mesmo que seja apenas reativo em resposta a relatórios, muito menos proativo. Agora, também discutimos com frequência que geralmente não são as partes contratadas que estão na sala que contribuem ativamente para a ICANN que estão menos

engajadas. Quando mencionei o apoio do setor, muitos dos que contribuem para a ICANN já estão comprometidos em fazer mais e estão ativamente engajados, geralmente são aqueles que não participam aqui e acho que o exemplo japonês é um exemplo, há registradores que não sabem o que eles podem estar fazendo aqui ou que eles têm um problema. Agora, isso pode ser uma questão de capacitação, é claro, mas também precisamos criar incentivos e aumentar o piso contratual e aqui voltamos a algumas das invenções que vieram debaixo, e Laureen agora nos guiará pelas lacunas vemos hoje e possíveis etapas futuras que nós, como GAC, podemos considerar.

LAUREEN KAPIN: Obrigado. Próximo e último slide. Eu sei que estamos um pouco ao longo do tempo. Então, novamente, os contratos formam o piso e acho que a conformidade da ICANN, e o painel concordaria que, se não estiver nos contratos, não pode ser aplicado. Então, a verdadeira questão é: o que está atualmente nos contratos? E há espaço para melhorias porque o poder de conformidade da ICANN emana dos contratos. Então, um dos lugares onde vemos uma disposição que está no interesse público compromissos do contrato de registro baseado em padrão é a proibição de distribuição de malware, abuso, infelizmente, botnets operacionais e você mesmo pode ler o banco, mas isso é diretamente do contrato de registro e você pode pensar à

primeira vista que isso significa, meu Deus, há todo esse comportamento que está sendo proibido, então, se isso acontecer, podemos simplesmente sair e aplicar contra isso. Mas na verdade não é isso que a proibição é. Isso é o que chamamos de requisito de downstream que apenas obriga os registros a dizer a seus registradores, as pessoas que estão lidando com os clientes que compram nomes de domínio, certifique-se de colocar em seus contratos com esses compradores que eles não podem fazer isso. se você estiver analisando os relacionamentos e as relações de aplicação, a ICANN e os registros prometem um ao outro que essa exigência de papel será incluída nos contratos com os registrantes, mas não há obrigação de os registros garantirem que os registrantes não fazem isto. Não há obrigação de que os registradores tomem certas ações, então essas são coisas e questões que devem ser discutidas na questão geral de como pensamos sobre as disposições aplicáveis sobre como responder ao abuso de DNS? E eu digo conversas porque não deve caber ao Comitê Consultivo Governamental isoladamente ou a qualquer grupo de partes interessadas isoladamente desenvolvê-las. Estamos identificando um problema, como responder ao abuso de DNS e qual deve ser a maneira de melhorar os contratos nesse sentido, mas isso tem que ser uma conversa com todos os grupos de partes interessadas, especialmente com as partes contratadas que têm sua realidade de negócios a enfrentar, eles sabem coisas que nós não sabemos.

Nós sabemos coisas que eles não sabem. Tem que ser um diálogo, então realmente nossa sugestão geral é que precisa haver boas conversas sobre isso para que possamos trabalhar juntos. Outro exemplo em que há uma lacuna potencial nos contratos trata das obrigações do registro de realizar uma análise técnica para descobrir se há ameaças à segurança, mas os contratos não dizem o que precisa acontecer depois que as ameaças à segurança forem identificadas. Então mais perguntas. E então o contrato de registrador padrão exige que os registradores investiguem prontamente e respondam adequadamente ao abuso de DNS, mas a Diretoria reconheceu que o contrato de registrador, o acordo de registrador básico, não define com especificidade o que isso significa, o que faz medidas razoáveis e imediatas investigar e responder adequadamente significa que houve discussões. Houve iniciativas voluntárias, há muito pensamento bom sobre isso, mas precisamos ter essas discussões que se concentrem nos tópicos amplos, como relatar e lidar com a resposta ao abuso do DNS e como os termos devem ser incluídos e implementados nos contratos, e executados.

LAUREEN KAPIN: Muito obrigada, eu sei que estouramos o tempo, peço desculpas, sei que havia mais perguntas.

MANAL ISMAIL: Obrigada a todos os palestrantes online, colegas do GAC pela ativa participação, o interesse da comunidade também, colegas do GAC, vamos voltar daqui a meia hora. Obrigada.