ICANN85 Mumbai | Fórum da Comunidade – GAC: discussão sobre atenuação do abuso de DNS
Segunda-feira, 9 de março de 2026 – 16h30 às 17h30 IST

NICOLAS CABALLERO Sejam bem-vindos de novo. Por favor, tomem seus assentos. Vamos voltar em um par de minutos. Obrigado.

JULIA CHARVOLEN Bem-vindos à sessão do GAC de Mitigação de Abusos do DNS, segunda-feira, 9 de março, às 16h30, hora local. Essa sessão é regida pelos padrões de comportamento e políticas anti-assédio da ICANN. Digam seu nome e o idioma que forem falar, se não for inglês. para termos uma boa interpretação e desativem o som dos outros dispositivos. Temos aqui o presidente do GAC, Nico Caballero.

NICOLAS CABALLERO Obrigado, Julia. Bem-vindos de novo à sessão de Mitigação de Abusos do DNS. Temos uma equipe maravilhosa hoje, a Martina Barbero, da Comissão Europeia, o Tomo Miyamoto, aqui à minha direita, também o representante do governo dos Estados Unidos, Gabriel Andrews. Susan Chalmers também. E temos o Sr. Devesh Tyagi, que é o orador convidado do ccTLD .in e Manju Chen, da rede de notificadores confiáveis. Será uma sessão de uma hora.

Teremos um Q&A no final. É uma troca. E passo a palavra à Susan Chalmers.

SUSAN CHALMERS Bom dia, boa tarde. Eu represento os Estados Unidos. Sou líder de tópicos sobre abusos do DNS. Estou aqui com meu colega do Japão, a minha colega da Comissão Europeia. Essa sessão do GAC e os abusos do DNS são um assunto prioritário para o GAC, devido pelo impacto dos ataques, os golpes com bot, phishing, etc.

E temos um plano anual, vamos mostrar, que está focado em duas áreas de trabalho. Temos a primeira área, fazer um acompanhamento do trabalho sobre a política da ICANN, sobre o DNS, os novos genéricos, e temos uma área de trabalho de capacitação, e isso é para gerar capacitação dos membros específicos do GAC.

O abuso do DNS tem a ver com atividades expúrias que os governos poderiam considerar como delitos como phishing, malware, etc., mas há uma definição muito específica para a ICANN, e porque para a ICANN, abusos do DNS significa malware, botnet, phishing, pharming, spam, como mecanismo de entrega.

Há três atores que têm a ver com serviços de nome de domínio que podem executar diferentes tipos de ataques, como provedores de internet, provedores de hosting, mas no GAC estamos focados no sistema de identificadores únicos e estabilidade e segurança do

DNS e dos identificadores únicos, isso com foco nas políticas para os registos e registradores com contratos com a ICANN.

Podem ser tomadas medidas de forma proativa para evitar que nomes de domínio sejam utilizados para fins espúrios. Em geral, os registradores e registrantes de gTLDs devem ter um contrato para a denúncia de abusos com auditorias de cumprimento e a supervisão dos requisitos dos contratos. Então, são dois aspectos da mesma moeda.

Essas obrigações quanto abuso do DNS foram estabelecidas especificamente através de emendas aos acordos ou contratos entre a ICANN e registradores que entraram em vigor em 2024. Aqui, um pouco de história, e vou fazer uma pausa. Temos, acho que são 19 representantes novos aqui no GAC, nesta reunião. Tem alguns deles aqui na sala. E não sejam tímidos, por favor. Levantem a mão.

NICOLAS CABALLERO Quantos estão aqui pela primeira vez? Países ou membros?

SUSAN CHALMERS Em geral, há documentos informativos que são distribuídos antes da sessão e os funcionários de apoio sempre coletam se um histórico sobre abusos do DNS, engajamento do GAC, que é breve, são 15 páginas para dar uma visão geral sobre a história que nós temos com esse assunto.

Aqui temos apenas os marcos e, para nós do GAC, para isso utilizado para recomendação, como por exemplo, da ICANN83 em Praga, e eu não vou lê-lo, ele está aqui na tela, mas isso é o que o GAC apresentou no ano passado em Praga. E mais recentemente foi adotado um novo estatuto de PDP para a verificação de domínios associados, isso foi a GNSO, e os meus colegas vão falar sobre as atividades em andamento a respeito desse PDP DC.

Vamos ver então, continuamos com a agenda. Antes e depois da atualidade. Na ICANN, recebemos duas apresentações diferentes para podermos entender diferentes iniciativas de políticas e operações que não estavam sob a incumbência da ICANN. Os colegas da Índia, a NIXI, que administra o ccTLD farão uma apresentação sobre como eles lidam com os abusos.

Na última sessão em Dublin, na ICANN84, recebemos uma apresentação dos notificadores confiáveis, Trusted Notifier Network, uma rede que tem a ver com a capacitação do plano anual do GAC. Essas redes, os TNN, são mais do que um programa, e vamos ouvir falar hoje, sobre a política e as estruturas do TNN através de Manju Chen. Então, passo a palavra ao anfitrião, o representante da NIXI, o senhor Devesh Tyagi, o CEO.

DEVESH TYAGI Boa tarde. A gente vem operando esse ccTLD desde 2012. Iniciamos várias iniciativas que queremos compartilhar com vocês baseadas nas experiências reais e concretas que tivemos com a NIXI. Essas são as iniciativas que nós estamos implementando atualmente.

Uma tem a ver com a verificação da chave ou a senha, nome do domínio, a verificação do WHOIS e a incorporação das autoridades da lei da Índia, porque recebemos várias sugestões a respeito disso. E, portanto, incorporamos muitas dessas ideias para mitigar o uso malicioso do DNS.

Então, primeiro, e começamos com o processo de verificação dos estrangeiros que estavam sendo incluídos no nosso registro .in. Então, para implementar isso, o registro .in verifica os registradores que utilizam documentos como passaportes, e carteiras de identidade de outros países, entre outros. Como temos um novo RAA, temos uma cláusula nova, a 4.4.15, em que os solicitantes estrangeiros que solicitarem um domínio .in devem demonstrar ter uma conexão comercial legítima ou um objetivo legítimo na Índia.

Esses são também alguns dos desafios que nós enfrentamos. Temos essas outras iniciativas que estamos levando à prática, começamos em outubro de 2023, monitorando o registro de nomes de domínio. Temos um monitoramento melhorado, através da implementação de medidas como limitar as palavras-chave, como GOV, entre outros, para evitar o uso malicioso deles. Isso também tem a ver com novas iniciativas do governo e também o nome de diferentes departamentos governamentais ou em nome deles, e foram incluídos nessa lista de monitoramento.

Fazemos uma verificação de todos esses nomes de domínio. Desde maio de 2024, implementamos o mecanismo em tempo real para

mostrar registros de domínios em bloco feitos pelos delinquentes em bloco ou em conjunto. Por exemplo, com o número de celular, que foi muito comum nos últimos anos, e também outras solicitações que podem vir de um número de celular, e isso de imediato é destacado pelo sistema.

Uma outra iniciativa tem a ver com a verificação manual do nome de domínio através de detalhes no WHOIS, porque às vezes temos diferentes registros que são errados e que estão ao mesmo tempo, e começamos a fazer uma verificação manual quando encontramos nomes de domínio suspeitos.

Atuamos sobre listas de nome e domínio que vêm de diferentes órgãos, como um centro de coordenação de cibersegurança, a CERT-In, por exemplo, entre outros. Também na nossa consulta observamos que algumas listas são reservadas e percebemos que estávamos gerando novas listas e decidimos ter uma reserva delas.

O monitoramento periódico dos registros de números do domínio começou em outubro de 2023, em que estabelecemos mecanismos de monitoramento periódico que verifica os domínios registrados e isso é verificado de forma sistemática. Isso tem a ver com o ciberdelitos, o phishing, e prejuízos potenciais para a reputação. E considerando o que a NIXI e a NET-in mencionaram e também as autoridades da lei, sabemos que há algumas atividades que poderíamos implantar como registros que querem ter o nome do governo. Portanto, há uma série de conteúdos que são indicados, uma alerta, há uma ameaça potencial. É feito um relatório à

instituição correspondente. Também com a RBI e CBI, porque muitos deles podem ser utilizados para uso indevido.

Este seria o mecanismo de implementação que estamos utilizando em tempo real para obter os números de telefones e acessar os e-mails. Utilizam os telefones, os celulares e os correios eletrônicos para identificá-los em tempo real. Então, através dessas iniciativas, eu quero compartilhar com vocês as estatísticas para que consigam ver como conseguimos, quais são os números associados à prevenção de atividades maliciosas, as notificações de ameaças são recebidas pelos organismos de aplicação da lei, do Centro de Coordenação de Cyber Crime da Índia, a CERT-In e uma verificação manual de eKYC.

Através dessas estatísticas de 2024, estamos recebendo 78 notificações, mas em 2025 isso diminuiu para 23. E agora, em 2026, apenas recebemos uma. Então, a iniciativa está sendo bem sucedida. Através do Centro de Coordenação de Cibercrime da Índia, que é um dos principais no país vemos o que aconteceu em 2023, 2024, 2025 e 2026, e foi diminuindo de 211 a 0 neste ano. Também quero dizer que tínhamos 506 em 2024, das notificações de ameaças, informada pelo CERT-In, que diminuiu a 177 em 2025, e este ano apenas 7.

Então, vocês conseguem ver a quantidade de incidências que foi reduzindo ao longo do tempo, dos últimos anos. Esta é uma iniciativa importante que estamos implementando, utilizando eKYC de forma manual e agora eKYC de forma eletrônica. Então

vemos aqui que aproximadamente se registram 3.000 domínios por dia. E através deste processo de verificação vemos que 4% são os domínios que conseguimos identificar como maliciosos. E depois que conseguimos colocá-los em espera para demonstrar ou confirmar se são realmente ameaças, apenas podemos fazer a verificação para um 4%.

Então 96% dos domínios podem ter sido criados para um uso indevido, mas tudo isso conseguiu ser mitigado por nós. Aqui estão os números e podem ver por si próprios. E através desta iniciativa, neste momento estamos no número de série 58 e avançamos muito bem. Está aqui esse número de série 58 de 4 milhões de domínios. Conseguimos identificar 2.276 como domínios com objetivos maliciosos.

Então, conseguimos um grande avanço. Mais uma vez, compartilho com vocês. Aqui temos o acordo de habilitação de registradores, que instruímos todos os registradores, inclusive os internacionais, para implementar requisitos obrigatórios KYZ. Também se colabora com os organismos de aplicação da lei durante os eventos internacionais, especiais, ocasiões sensíveis, para ter a certeza de que existe uma preparação contra a cibersegurança.

Também desenvolvemos procedimentos e padrões estándar ou padrões equilibrados a nível I4C. Com essas iniciativas, tivemos muito bons resultados. O novo acordo de habilitação de registradores fez com que o nosso domínio .in seja mais seguro. E, por sua vez, vemos que temos obrigação de utilizar eKYC para

todos os registratários, se mantém o registro de transferências financeiras, que é feito pelos registradores, se faz reclamação também.

E também há um representante local com um escritório com base na Índia. Com todas essas medidas, conseguimos mitigar a possibilidade de que se registrem domínios com finalidade maliciosa. Quero agora compartilhar os resultados. Inclusive, o Alto Tribunal de Delhi viu os benefícios deste processo de verificação que implementamos com o eKYC. E o Tribunal disse que aumentou a transparência porque existe um processo estruturado, implementado pelo NIXI, e realmente isso é beneficioso para todos. Os organismos encarregados de aplicação da Lei da Índia também valorizam o apoio que dá a NIXI para poder parar o cibercrime no país. Isso é o que eu queria compartilhar com vocês e agradeço pela oportunidade de falar.

NICOLAS CABALLERO: Muito obrigado. Temos de 3 a 5 minutos para perguntas por questões de tempo. Vamos dar prioridade aos governos. E caso não existam perguntas dos representantes dos governos, podemos passar a dar a possibilidade a outros participantes. Não vejo nenhuma mão no Zoom. Veremos se há perguntas aqui na sala para o senhor Devesh. Por favor.

NÃO IDENTIFICADO Eu sou representante de um registrador e eu queria saber o que é que querem dizer quando falam de relatórios de ameaça?

DEVESH TYAGI E relatório de ameaça basicamente tem a ver com os organismos de aplicação da lei, com as suas próprias ferramentas, analisam os domínios de forma diária. Os registros de .in compartilham todos os domínios criados a todos os organismos de aplicação da lei do país e, através dessa ferramenta, analisam esses domínios criados e nos apresentam um relatório de ameaças.

NICOLAS CABALLERO Obrigado. Está Taipei Chinês?

PEI YING Eu também trabalho com o TwNIC e queria pedir que compartilhasse mais a sua experiência com respeito às medidas que implementaram, se fazem parte das leis nacionais, ou se são voluntários para que as organizações cumpram.

DEVESH TYAGI Claro que estamos muito satisfeitos compartilhando nossas experiências com vocês. Nós nos guiamos pela legislação da Índia, mas também por outras iniciativas, porque anos anteriores, apenas respondíamos às ameaças. Agora tentamos fazer um trabalho preventivo antes de que a ameaça apareça. Então, esses resultados que compartilhei dos 3.000 domínios registrados,

identificamos 4% como os maliciosos e 4% desse número, por sua vez, apenas essa percentagem podemos comprovar que são usos maliciosos.

NICOLAS CABALLERO Muito obrigado. Vamos ver se há alguma outra pergunta. Vamos dar prioridade aos representantes dos governos para que façam suas perguntas primeiro.

BANGLADESH Obrigado. Eu sou representante do Bangladesh, do GAC. Tem uma muito boa iniciativa na Índia. Com a análise das ameaças dentro da Índia, vocês obtêm informações sobre o uso indevido do DNS e estão tomando algumas medidas. O que acontece com o uso indevido do DNS por parte de registros que estão além do .in. Recebem também informações de forma periódica a respeito deles e o que é que fazem? Que medidas tomam?

DEVESH TYAGI Hoje apenas estamos falando destas modalidades com os níveis mais altos. Estamos trabalhando para mitigar também essa situação.

NICOLAS CABALLERO Obrigado ao Bangladesh pela pergunta. Vejo uma mão ali. Podemos receber uma pergunta a mais.

MELANIE ALDONCE: Sou Melanie Aldonce, do Chile, para os registros. Muito obrigado, doutor Devesh, pela apresentação. Quero consultar se analisam domínios que estão registrados, mas não ativados de imediato, ou seja, que não são associados a um host, porque sabemos que muitos dos domínios que fazem uso indevido estão registrados e permanecem ativos durante muito tempo.

DEVESH TYAGI: É uma pergunta muito clara que está fazendo. Estamos sabendo, estamos muito conscientes dessa situação. Hoje compartilhei um processo, e este processo foi se tornando automático. Todos os meses, com a ferramenta que criamos, temos a chance de executar essa ferramenta para analisar todos os domínios que têm o registro. E aí geramos um relatório que também é compartilhado com os organismos de aplicação da lei, porque sabemos que há alguns domínios que podem se tornar ativos depois de um tempo. Então, todos os dias ou todos os meses, analisamos esses domínios que foram criados utilizando ferramentas automáticas, identificamos e depois reportamos aos organismos de aplicação da lei.

NICOLAS CABALLERO: Muito obrigado. Julia?

JULIA CHARVOLEN Não há pergunta, mas eu vou ler uma pergunta do chat. do Thiago, vice-presidente. Quantos registradores estão comercializando o ccTLD .in e conseguem ver as registrações maliciosas referidas a um ampla leque de registradores ou apenas de uns poucos?

DEVESH TYAGI Basicamente, cada registrador está tendo algumas atividades através dos domínios que se registram através deles. Então, para os registradores estrangeiros, vemos a filiação com o .in. E para todos os outros registradores da Índia, não entramos nesses detalhes. Cada vez que há uma registração com o registratário ou registrador da Índia, e eles utilizam esse domínio especial com KYC, que é o requisito que estabelecemos.

NICOLAS CABALLERO Muito obrigado. Continuamos, então. E, neste momento, vou passar a palavra à Martina Barbero, da Comissão Europeia, e a Gabe Andrews, do FBI, que vão apresentar um relatório sobre os debates de política do uso indevido do DNS.

MARTINA BARBERO Muito obrigada. Mando um abraço daqui. Desculpe por não estar ali. Vamos falar do que estamos falando nas deliberações do PDP. Seguinte slide. Desde o lançamento do PDP, como menciona Susan, na parte de introdução desta sessão, começamos a formalizar as formas em que trabalha o GAC, estabelecendo um

grupo reduzido e específico para o uso indevido do DNS, que é a forma que nos preparamos para as deliberações do PDP.

As ideias para formalizar esse grupo também cumpre tudo o que tem a ver com os dados de registração para ver se havia alguma falsificação e nós trabalhamos de forma periódica com os representantes do PDP do GAC, tanto -- como eu, temos essa posição no PDP e vamos ter muito trabalho com esse PDP sobre o uso indevido do DNS e estabelecemos esse grupo que consideramos que era uma boa ideia para ver de que forma podemos estar presentes na discussão, mas para utilizar toda a lista de distribuição do GAC, o que talvez seria um pouco abrumador para alguns.

Então, agora temos no GAC 17 participantes. O grupo está aberto para aqueles que querem participar. Neste assunto do uso indevido do DNS, podem se unir enviando uma informação, uma nota, um formulário para o grupo de apoio para ver quem quer formar parte. E há também outras pessoas que faz tempo que estão trabalhando no tema.

Quando mencionou, Susan, o lançamento do PDP foi já decidido pelo Conselho da GNSO no mês de dezembro e a primeira reunião do grupo, do PDP, se realizou há dois dias. Hoje é primeira vez que se reúne aqui na ICANN85. Está no PDP 1, vinculado com verificações de domínios associados, que tem a ver com o relatório apresentado no verão passado.

E o segundo PDP fala da medida de proteção para acesso aos novos clientes e não sabemos quando será ou começará esse PDP. Para o primeiro temos uma delegação que tem dois membros do GAC, que somos eu e Gabe, que vem da Comissão Europeia e do FBI, que são vice-presidentes do --, e também Wolfgang, da Alemanha, é um participante, pode participar das discussões, mas não tem direito de voto. Ele provém da polícia e também está da polícia da Grécia, mas, nesse caso, é um substituto. Caso, perante a ausência de Gabriel e eu, pronto, eles, neste momento, atuam como substitutos e não tem voz nem voto.

É um grupo bastante forte, tem bastantes participantes que são membros do GAC, e isso é muito útil. A primeira reunião, as primeiras se realizaram dois dias atrás e ontem. No seguinte slide vou mencionar um pouco o que discutimos nessas duas primeiras sessões. A ideia dessa reunião inicial, que foi agregada na ICANN85, foi receber informações sobre os prazos do trabalho.

E aqui vemos no slide os principais marcos. O relatório inicial do PDP, esperado para fevereiro de 2027, o final, esperado para setembro, e a GNSO considera o relatório final para outubro, novembro de 2027. Hoje recebemos uma apresentação de especialistas e como eles fazem verificações associadas e as melhores práticas.

E o mais importante para vocês lembrarem é que vamos ter que oferecer comentários iniciais antes de 20 de março. Temos a ICANN85 até a quinta-feira, e depois vamos começar a preparar o

comunique do GAC, temos um documento vivo no Google Docs, em que os comentários poderão ser fornecidos para os diferentes membros, e continuamos trabalhando no documento, nesse pequeno grupo, para assegurarmos de poder ter um prazo de imediato.

GABRIEL ANDREWS

Para que vocês saibam, essas são as perguntas que serão fornecidas no gráfico do PDP. Para dar respostas, isso vai ser, como a Martina mencionou, semana que vem, sexta-feira, para que avancemos no PDP. E o presidente aqui, Paul McGrady, vai tentar cingir-se aos termos, e vamos oferecer respostas, mas respostas preliminares, em algum momento da semana que vem, e não podemos ter mais tempo para uma revisão.

Temos um grupo pequeno que está trabalhando de forma colaborativa na redação das respostas a essas perguntas. Vamos ver o futuro agora. O PDP antecipa o acesso aos apps. Pelo que lembramos, a ICANN publicou também o Infermal, um relatório associado. É uma associação, uso da API, é uma base firme, legal. E isso está em qualquer relatório, esperamos poder participar disso, antecipar o trabalho.

E, além disso, o GAC registrou nas últimas conversas, passadas em documentos, que temos mais considerações de áreas potenciais sobre um PDP com um escopo mais limitado que possa incluir um monitoramento proativo, medidas preventivas, resolução de problemas, como phishing, entre outros, em que um domínio pode

ter diferentes domínios e subdomínios e também nomes criados para corporações também, outros como siglas também, e o DGA, por exemplo, esse é o algoritmo de geração de domínios e todos eles são potencialmente exploráveis até o futuro. Passamos a palavra ao Tomo.

NICOLAS CABALLERO Temos alguém da Comissão Europeia, Gemma.

GEMMA CAROLILLO Muito obrigada, Nico. Vou ser breve. Primeiramente, parabéns aos colegas do GAC, que participaram com seus comentários, comentários realmente significativos. Eu gostaria de destacar aqui, em benefício da informação dos colegas do GAC e também do presidente do PDP, que seria muito bom que o grupo do PDP revise. E, novamente, o estatuto para encurtar o prazo esperado ano, ano e meio, e mesmo com o relatório inicial e também reuniões semanais e trabalho preparatório, é pouco, porque isso requer recursos intensos de todas as comunidades e profissionais envolvidos, para fazer com que o escopo seja menor e não controverso. Então, é isso que nós encorajamos, que o estatuto do PDP, revise os assuntos de preocupação que têm a ver com os prazos. E também suas opiniões, e também da GNSO, sobre outras questões, é importante que sejam discutidas nesse relatório, enquanto a metodologia, questões com muitas prioridades, como a transparência, endereçamento, acurácia de dados, etc.

NICOLAS CABALLERO Obrigado, Comissão Europeia. E a vez da Índia.

SUSHIL PAL Obrigado, Sr. Presidente. Eu sou o Sushil da Índia. Aqui, parabéns aos líderes do GAC, encarregados disso. Eu sou Sushil Pal. E destacar a importância de outras áreas com problemas prioritários, monitoramentos, implementar medidas sobre a validação paralela, tomando medidas preventivas, e a validação paralela de dados e registrantes com um registro. É muito importante, sei que há preocupações também na GNSO que deveria trabalhar, e está trabalhando, tentando acelerar o processo. Isso para evitar que os ciberdelinquentes prosperem. Isso antes de 2027. Temos uma metodologia aqui no nosso país. Aqui o Sri mencionou e é muito bom mencionar o que podemos fazer com esses registrantes que estão fora de um domínio, do nosso domínio. É importante considerar este período de validação, um período de 15 dias. Deveríamos eliminá-lo para resolver o problema, mas o GAC deve considerar emendas nos contratos assim que possível.

NICOLAS CABALLERO Obrigado, Índia. Então, vamos continuar. Tomo Miyamoto vai falar sobre as redes de notificadores confiáveis. Vamos para a próxima.

TOMORI MIYAMOTO

Primeiro, eu vou mostrar novamente o plano anual e o comuniqué. Isso vem já da ICANN 84. E aqui o que queremos fazer é avançar o PDP, como a Martina e o Gabriel mencionaram antes. Também a capacitação, que inclui os 20 novos membros do GAC, e não só eles, mas também compartilhar as melhores práticas que poderiam contribuir para a mitigação de abusos, e isso está presente na cláusula 4.7.

A questão dos contratos, o que vemos aqui na caixa verde. Em verde, vemos o contrato da ICANN, bastante limitado e a definição de abuso do DNS, que também é limitado, como o botnet, o spam, mas o processo é bem mais amplo, E precisamos de expertise, sim, porque esse é um problema. E precisamos de mais flexibilidade, além da incumbência do texto contratual da ICANN.

MANJU CHEN

Diretora da Rede de Notificadores Confiáveis. Essa é uma breve apresentação do que fazemos. Depois teremos o Q&A. Vocês ouviram nas apresentações em Dublin, sobre o Edmund e planos diferentes. Estamos baseados no mesmo conceito e com base nesse mesmo conceito, pensamos que os contratos de identificadores são lentos demais e queremos construir uma rede para que vocês façam parte dela e vocês sejam também notificadores confiáveis, que suas notificações sejam confiáveis também por todos os intermediários.

Temos muitas ccTLDs e os APAC que estão muito interessadas e já estão pedindo para registrar-se, inscrever-se. E também há muitos

gTLDs no mundo e muitos deles estão demonstrando um grande interesse. Essa é uma das maiores diferenças entre todos nós. Queremos cobrir mais de 200 TLDs.

Então, pelo menos 60 dos domínios atuais estão recebendo interesse e atenção daqueles que querem tornar-se notificadores confiáveis também. Temos registos da ICANN, mas não temos intermediários. Temos comércios, empresas, marcas que têm um custo injusto por sofrer ataques de phishing, ciberataques, e não têm nem tempo, nem expertise para resolver esse tipo de problema.

E, então, devem terceirizar a solução ou desativar o sistema. E isso com intermediários. Enviam notificações gratuitamente a intermediários. Isso é gratuito. Enviam tantas quanto possível. E também são pagos por enviar notificações. E os intermediários estão aqui considerando esse conceito de responsabilidade social, e se eles retirarem esse domínio de acordo a esse pedido, devem prestar contas à sociedade ou aos clientes.

Então, para diminuir esses custos, é necessário ter critérios mais estritos para reduzir os custos. E o que percebemos é que isso faz com que todos estejam insatisfeitos, porque é um sistema injusto. A maioria de vocês pode sentir-se identificado com essa situação, porque tem muitos ataques e muitos golpes de cidadãos, que você sente que não estão fazendo o suficiente e que deveriam trabalhar com mais velocidade.

Isso tudo é gerado pela inteligência artificial, não pertence a nenhum país, mas os governos também estão pressionados. E se não se respeitam suas necessidades ou resolvem, sentem que devem provar novas regulamentações para lidar com este assunto. Então, todos colocam a culpa no outro.

A nossa solução, queremos reduzir o custo e o risco para os intermediários da internet, para que se sintam à vontade e com mais segurança quando fazem uma retirada de um domínio através de um pedido. E como fazemos isso? Para isso, precisamos melhorar a detecção e a retirada. Temos que melhorar a qualidade e a exatidão das solicitações.

Então, dessa forma, podemos desenvolver a concorrência necessária. E também falar com os governos, e por isso que estou aqui, porque os governos são importantes. Eu agradeço pelo convite, mas temos que trabalhar de forma conjunta. E também quero mencionar as políticas da nossa rede, porque apontam a nos levar a um processo que possa ser multiplicado.

Queremos que todos comentem se estão interessados. Posso compartilhar a questão da política, o documento que se refere à política. E vocês podem dar a sua opinião. E, finalmente, mas nem por isso menos importante, isso sabemos que não acontece a nível do DNS apenas na ICANN. Temos um alcance bastante limitado centrado no DNS, mas isso acontece em todas as partes, e para combater o uso indevido no mundo atual ou em linha, precisamos da cooperação em todos os níveis da indústria.

Esses são os objetivos que queremos cumprir. Que os notificadores tenham que verificar as suas notificações antes de enviá-las à seguinte entidade. Depois os intermediários. Queremos também que os notificadores estejam autenticados para que sejam confiáveis. E uma vez que conseguem essa situação, status de confiável, temos, então, algum critério para estabelecer essa estabilidade, mas, se querem falar mais a respeito, podemos depois falar.

Queremos reduzir os riscos, os riscos legais, especialmente para os intermediários, para que se sintam mais seguros na hora de agir quando manejam as solicitações de retirada. Então, queremos ter um contrato que permita que os intermediários possam sentir essa segurança de que podem agir, e para isso teríamos uma cadeia de contratos.

Os notificadores confiáveis têm que aprovar uma série de requisitos e as suas notificações são enviadas a TNN com determinados critérios que devem cumprir conforme a --, não é o que eu mais gosto, mas é o que se aplica. Tem que estar verificados. Também não devem estar automatizados, serem -- e exatos. Esta é a descrição que utilizamos, devemos continuar o devido processo, devem cumprir, para verificar as solicitações, devem cumprir todo esse processo. Por isso é que confiamos nesta solicitação e também entre os notificadores, se existir a confiança. No próximo slide, vou explicar um pouco mais.

As notificações estarão padronizadas e codificadas para facilitar as coisas a todos e todas, para que não tenhamos inconvenientes, com não ter evidência, só não saber qual é a solicitação, de que trata, e devido a essa cadeia de contratos ou de confiança, os notificadores vão conseguir verificar essas notificações que recebem, ou que recebam. Na verdade, aqui a intenção é investir na transferência de custos. Eu vou explicar como aplica isso aos organismos de aplicação da lei.

Seguinte slide. Os organismos de aplicação da lei, nós vemos de outra ótica, porque os requisitos para os notificadores confiáveis poderiam ser difíceis de cumprir para estes organismos. Conhecemos alguns organismos, talvez não podemos ter contato com todos, mas todos os organismos oficiais de aplicação da lei são considerados notificadores confiáveis, devemos verificar as solicitações recebidas por parte desses organismos.

Por questão de tempo, talvez não consiga explicar como fazemos a revisão dessas notificações, mas há duas condições. Quem quer se incorporar a esses organismos de aplicação da lei deve reconhecer que as notificações devem cumprir as normas da indústria para garantir a diligência do procedimento e também tem que apresentar uma condição indene ao TNN aos intermediários quando querem, assim, trabalhar com a nossa organização ou chegar até a nossa organização.

Aqui é o que Tomo antes descreveu. Temos que identificar todos nessa rede, mas a ICANN tem um alcance limitado a respeito. Nós

começamos com a ICANN, mas no futuro esperamos poder ampliar e chegar a outros atores do mundo real, as empresas de telecomunicações, as de web, as que se ocupam de nomes, de números e cibersegurança. Com isso, termino a minha apresentação e fico à disposição para perguntas.

NICOLAS CABALLERO Infelizmente, não temos tempo para uma troca de opiniões, mas quem quiser pode entrar em contato com Manju e sua equipe de forma direta daqui a pouco. Agora quero passar a palavra a Tomo para alguns comentários finais referidos com o comunicado do GAC e uma sugestão a respeito.

TOMORI MIYAMOTO Muito obrigado. Quero passar o microfone assim que possível, mas temos aqui três PDPs ou três assuntos para considerar que são importantes, que é o desenvolvimento da política de verificação de domínios associados, o futuro desenvolvimento de políticas sobre o uso indevido do DNS, também temos o PDP 1. E um prazo para o PDP 2. Também existem outras brechas que foram identificadas. E também temos que considerar as possibilidades para futuras iniciativas e colaborações. Para trabalharmos no âmbito do uso indevido do DNS. Então, deixo aberto o microfone para escutar as suas sugestões. Obrigado.

SUSHIL PAL

Era um comentário, mas como há um slide específico sobre o comunicado, quero então saber se podemos incluir esse aspecto do mecanismo de prevenção a respeito do período de registros, ou para a registração?

SUSAN CHALMERS

Eu acho que a respeito desta sugestão, o PDP atual e os futuros PDPs poderiam aceitar, digamos, essa sugestão, incorporar essa sugestão. Eu acho que existia um ponto no relatório de assuntos referido a isso. Se falava de uma metodologia para priorizar diferentes áreas para o trabalho futuro, então talvez ali poderíamos incorporar esse tema. mas sem dúvidas que vamos passar por um processo para compartilhar o texto correspondente a esses temas de importância.

SUSHIL PAL

Obrigado, Susan. Entendemos que isso foi mencionado, mas também surgiu como uma das questões de importância em outras sessões de redação do comunicado. Então, eu acho que isso é uma coisa muito clara, tentamos tornar mais expeditivo o processo para que permita a verificação dos nomes de domínios associados. Resultados que estamos esperando faz um ano. Esta medida preventiva vai ter um impacto maior que o que poderíamos ter com o processo de PDP, referidos com os nomes de domínios associados. Eu acho que esta medida preventiva deveria ser transmitida à diretoria como uma recomendação para que

encontrem as modificações contratuais necessárias através da forma ou meio necessário também.

NICOLAS CABALLERO Obrigado, Índia. Vamos tratar em outra sessão de redação do comunicado. Ficamos sem tempo. Não sei se querem fazer algum comentário final.

SUSAN CHALMERS Há várias reuniões dos responsáveis dos temas do GAC convidaram a maioria dos países que têm ccTLDs a fazerem as suas apresentações. Temos .rw para Ruanda, como já vimos em Kigali, e agora também, no caso, temos outro, mas aqueles que são novos neste tema. Também temos o espaço de gTLD, que são bem diferentes e muito exclusivos dentro da ICANN. Há um processo multissetorial que pode obter informação a partir das práticas nacionais, mas são processos especiais, separados, singulares e, no final das contas, é necessário da comunidade e de todos os envolvidos. Queria destacar que, para aqueles que são novos, esses são dois espaços de política separados. Era isso que eu queria dizer apenas e eu quero agradecer a todos por sua participação neste processo.

NICOLAS CABALLERO Obrigado, Estados Unidos. Índia, pediu a palavra de novo. Não? Ah, dou por encerrada. Obrigado, Devesh, Tomo, Susan e todos os participantes aqui. E nos encontramos amanhã, 9 horas, para a

reunião com o ALAC. Obrigado e aproveitem a merenda, os drinks ou o jantar. Obrigado.