
ICANN71 | Fórum virtual de políticas – Discussão do GAC sobre atenuação do abuso de DNS
Segunda-feira, 14 de junho de 2021 – 14h30 às 15h30 CEST

GULTEN TEPE:

Vamos começar. Bem-vindos a Sessão do GAC da Reunião 71 da ICANN sobre a Mitigação do Uso Indevido do DNS. Para economizar tempo, não vamos nomear todos os assistentes e os membros presentes vão estar inscritos nas atas. Queremos lembrar que, por favor, escrevam seu nome e a quem representam, quando ingressam na sala de Zoom. Se querem fazer comentário ou pergunta, por favor, escrevam QUESTION ou COMMENT entre colchetes, para que todos os participantes possam vê-lo.

As sessões do GAC vão ter interpretação simultânea nos 6 idiomas da Nações Unidas e português. Podem fazer o uso no Zoom da barra de ferramentas, onde diz quais são línguas que podem escolher. Se quiserem falar, levantem a mão na sala do Zoom. por favor, digam seu nome para os registros. Ao falarem, indiquem o idioma, em que vão falar, se não for inglês. Por favor, falem de forma clara para ter uma interpretação correta. Então, vocês vão encontrar o link no chat. Por favor, silenciem seus dispositivos e notificações, para evitar problemas. Isto posto, passo a palavra a Manal Ismail.

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, PRESIDENTE DO GAC: Obrigada, Gulten. Damos as boas-vindas. Temos uma sessão agora, de 90 minutos, onde vamos falar da mitigação do uso indevido do DNS. Esperamos em 60 minutos e podemos terminar, então nesse prazo. Depois vamos ter 30 minutos para falar sobre o Comunicado. E comunicar, debater algum dos temas, que podem estar incluídos no Comunicado, bem como aqueles que possam redigir. Eu vejo que já temos uma lista longa de oradores. Enquanto o trabalho de segurança pública do GAC, o nosso colega japonês também convidou pessoas do Grupo de Trabalho de Abuso de Mensagens [inaudível - 00:02:35] e móveis. Sem outros assuntos, introduções, quero saber quem vai começar. Laureen? Muito bem.

LAUREEN KAPIN:

Eu sou das copresidentes do Grupo de Trabalho de Segurança Pública do GAC. Também está comigo, Chris Lewis-Evans, como copresidente. E o colega também do FBI, Gabriel Andrews, que está acordando e levantando muito cedo, como outras pessoas também. Eu sei. Para este tema, temos convidados especiais, Shinya Tahata do Japão e também, convidados... outros convidados, que vão apresentar o seu estudo sobre o ingresso, a registo de dados de domínio.

Bom, muito bem. Como Manal pode ser, peço desculpas antes de começar. Se pegamos mais tempo, se superamos o tempo desses 90 minutos. Mas eu acho que a ideia é que todos possam entender do que é que estamos falando. E deixamos as perguntas em geral para a última parte. A não ser a apresentação de MAAWG, da nossa colega do Japão. Talvez queiram responder as perguntas no final das suas

apresentações. Então, vamos começar com o que devemos. Como já foi dito, o uso indevido do DNS é um dos temas sobre os quais voltamos todas as reuniões, porque é muito importante. É um assunto que é, na sua maior parte, vemos nas notícias todos os dias, ameaças a infraestrutura crítica no âmbito financeiro. Isso faz um impacto na vida diária das pessoas, onde pode haver roubo de identidade. E também esses malandros utilizam o DNS para realizar os seus crimes.

Vamos falar sobre diferentes assuntos, que tem a ver com o uso indevido do DNS e também de que maneira, como comunidade, podemos mitigar esse uso indevido. Também haverá um relatório atualizado sobre um documento de SSAC, que o FBI vai apresentar de um trabalho em colaboração, que realmente fez com os nossos colegas das partes envolvidas e que tem a ver com o uso indevido, temas associados como *Botnet* e o uso malicioso. Também vai se falar sobre a quantidade de tempo, que leva responder aos pedidos de dados de registro. Nós sabemos que essa informação pode ser fundamental, essencial para os pesquisadores. Porque às vezes, querem fazer explodir o DNS.

Também vamos falar sobre recomendações da equipe de revisão, confiança, escolha dos concorrentes e concorrência. Depois vamos falar sobre registratários, em realidade, registradores e a que partes devem recorrer e não. Aqueles que ainda não tenham a informação, que estão procurando. E depois, os nossos colegas do MAAWG vão falar também... também a colega do Japão, é cumprimento contratual, que é um dos elementos-chave. E depois veremos quais os passos futuros. A agenda está bastante completa. É um menu completo, portanto

vamos para o primeiro prato desse cardápio. Vai falar agora, vamos falar então, agora.

Não nesse slide, porque fala basicamente do programa. E em verdade, a ICANN deu muita, passou muita informação sobre os eventos, que vão realizados sobre esse assunto, sobre esse tema. então, Chris, por favor, fale um pouco sobre o relatório do SSAC.

CHRIS LEWIS-EVANS:

Obrigado, Laureen. Bom, vou falar sobre esse documento SSAC 115, que tem uma abordagem Interoperativa para poder solucionar o manejo, gerenciamento abusivo do DNS. Tem um quadro proposto, que abrange grande quantidade de documentos. Muitos desses documentos resultam, mais interessantes para nós, o SWGO para política. E o primeiro tem a ver com o ponto primário de contato para resolver esses casos de abuso indevido. Uma das coisas com as quais lutam as autoridades é ver como chegar a uma resolução desses problemas e como se vê na indústria em geral. Às vezes, o que acontece é que em lugar de... para o lugar adequado, são enviados anúncios de... ou advertências de uso indevido. E só a gente tem a possibilidade de ver isso. Então, o ponto primário tem que criar um lugar único, para que todos os pedidos vão para lá. E ter o ponto de contato certo para chegar à resolução. Depois temos os caminhos de escalamento.

No sentido de que se quer ir ao ponto, que tenha uma relação direta com a entidade, que está gerando esse uso indevido. Às vezes, não respondem. Então temos esses caminhos para ir escalando na hierarquia e poder ver como elevar esse pedido para chegar a quem

corresponde e obter uma resposta. É claro que também há um cronograma vinculado e com esse caminho. E também sei que alguns membros do SSAC não estiveram de acordo com algumas das propostas realizadas no SSAC 115. Uma teve a ver com isto, os caminhos de escalamento. Quais seriam os períodos que se davam para passar de um degrau para o outro. Alguns pensaram que não era a velocidade certa. Isto foi algo que foi colocado. Então igual, acho que é muito melhor do que podíamos ter esperado. As autoridades, o que querem fazer é garantir que temos normas também, porque pensam que é bom ter normas, que estejam normalizado com padrões, que falem sobre diferentes faixas de pessoas, que participam e ver quais são as que manejam o tema do uso indevido do DNS. E reduzir assim, a carga de algumas outras entidades, que recebem solicitações todos os dias.

Depois o tema da terminologia, da evidência das normas que também tem a ver com os caminhos mencionados antes, como se faz essa elevação do pedido. É algo que abrange vários pontos e que tem a ver com disponibilidade e qualidade da informação de contato. Se essa informação é a quem se deve dirigir realmente, vamos obter o resultado que queremos, nos dirigindo a esse contato. Então devemos pensar nos revendedores de um lado. E há outro aspecto, que são os dados reais, que se... e que são recebidos para ver se esses dados são certos ou não. E permitem tomar as ações mais adequadas e convenientes. Isso... esse foca então, em apoiar tudo, o que se propõe. Mas é claro que o mais importante é o tema do contato e esses caminhos de escalamento.

Dentro do SSAC 115 surge com essas recomendações de múltiplas partes, é que é necessário um pouco de consideração de que o uso indevido do DNS não está limitado a comunidade da ICANN. E como a ICANN pode começar uma conversa e mostrar na indústria, quais as melhores práticas, porque devemos considerar, que são vários os atores, que intervêm. Como já disse, no PSWG, a proposta é ter um facilitador comum do uso indevido, como é aqui chamado, para resposta aos pedidos. E comece, essa pessoa iniciar a conversa e ver como se pode implementar. E tivemos diálogo com várias partes. E todos dizem que seria bom ter essas conversas com uma pessoa. E eu gostaria de ver isso no futuro.

Sabemos que o GAC viu isto como algo que... ao qual podemos... que podemos apoiar. E realmente, realizar contribuições sobre como poderia funcionar dentro de cada uma das jurisdições. Temos que ter presente, então tudo isso. E vou passar a palavra para o Gabriel. Obrigado.

GABRIEL ANDREWS:

Eu vou me dedicar, vou dedicar 10 minutos a falar do quadro do contexto do DGA e o que tem a ver com o software malicioso. Esses é um projeto entre o Grupo de Trabalho de Segurança Pública e o registro. Realmente, falamos e também temos a oportunidade de definir. Quando dissemos DGA, isso é algo técnico. E tem a ver com os *botnets*. Os *botnets* são redes, que comprometem os dispositivos que são controlados por delinquentes. Alguns dos maiores que tivemos, tem a ver com avalanche.

E se estão controlados, utilizam esses algoritmos, que geram domínios, os DGAs. Esses algoritmos são um código, uma ferramenta que pode ser utilizada para ingressar uma data, para um momento específico. A ação que tomaram as autoridades contra os *botnets* é algo que tem a ver com que são baixos em frequências. Mas o seu impacto é alto. Quer dizer, que podem dar uma ação muito ampla. Todos os domínios vinculados com o DGA podem ter um impacto administrativo, tanto nos registros em que participamos, quanto nas autoridades com as que participamos. Temos centenas de milhares de domínios vinculados com o DGA. E as autoridades antes tinham que ir as autoridades para atualizar, quais eram os domínios vinculados com esse DGA. É realmente, isso se faz ano após ano. Os tribunais têm que investigar isto. Os registros realmente não queriam que... ir a ICANN para solicitar dispensa para solicitações feitas por essas solicitações.

E esse quadro se fez com a possibilidade de fazer uma derivação desses DGAs para um só. Essa é uma ação perene. É... seria uma ação, que perdura durante toda a vida, durante toda a vida do DGA. E não ter que fazer os registros todos os anos, uma nova solicitação para essa dispensa na ICANN. Esse marco, esse quadro é voluntário. Não é vinculante. As partes interessadas de segurança pública querem que os entendimentos, aos quais chegemos de forma comum, sejam úteis para estabelecer o processo futuro de todas as partes. Os registros, as partes, todos os que têm que tomar uma ação responsável para evitar todos esses DGAs. Isto posto, queria pedir a James Galvin para saber se ele tem algumas palavras dentro da sua representação do Grupo de Registros ou como representante do Grupo de Registros.

JAMES GALVIN:

Muito bem. Eu queria falar de que o marco do uso indevido do DNS é importante. Eu sei que... desculpem, esta é a imagem que eu queria apresentar no anterior, porque não está na sequência. O marco, então do uso indevido do DNS é uma coisa que inclui muitos aspectos. E tem a ver com o SSAC 115, como falou Chris. O marco também como falou Gabriel. Então, esse quadro fala do ecossistema legal, ao qual faz referência o SSAC 115. Vocês podem ver aqui, à direta, que o sistema de registo, onde temos registros e registradores são uma parte pequena desse ecossistema. Estas são as coisas sobre as quais podemos agir. Então o que faz esse contexto é trabalhar sobre o uso indevido do DNS. E isso faz com que os registros e registradores podem acessar ou trabalhar dentro desse quadro. Mas esta outra partezinha, que aparece aqui, é apenas um elemento de todas as coisas, que são aplicáveis aos registros em particular. E esse é o espaço, no qual nós podemos agir de forma rápida e específica para solucionar esse tipo de inquietações. Mas como diz o SSAC 115, quando foi adotado oportunamente, foi trabalhado por diferentes partes contratadas e também foi reconhecido para ambos os grupos de partes interessadas. Se bem, é voluntário. Diz que há muitas pessoas que fazem parte do ecossistema, mas não estão presentes.

Se pensamos no SSAC 115, nós achamos ou falamos das ações, do tempo necessário. Mas a ideia é ver como fazemos com que tudo funcione dentro dos registros e dos registradores. O problema é muito mais amplo do que nós podemos fazer no nosso próprio espaço. Existe a necessidade de ter um facilitador comum, que é aquele que menciona

o SSAC 115. Porque há muitos outros atores, que estão por fora do sistema de registro, que não fazem parte desse trabalho e eles também fazem parte do trabalho.

Muitas das ações e dos programas, quando falamos do SSAC 115 e como ter um facilitador para respostas, tem a ver se vamos ver a pessoa indicada no momento certo. Os registros têm algumas ações, que podem tomar em algumas circunstâncias. Nós, como registradores, fazemos parte e temos que fazer a derivação as partes adequadas. Mas talvez seria mais fácil, se diretamente encaminham-se os pedidos a essas partes, que têm que definir. Essa demora, então em responder ao uso indevido, a respeito da ação que tem que tomar, tudo tem a ver com o que as partes a serem tratadas ou conectadas ou contatadas sejam as devidas. Eu falo, então em nome do Grupo de Partes Contratadas.

De qualquer forma, os registros estão trabalhando de forma direta com o PSWG, do Grupo de Parte Interessadas do Registro. O PSWG faz parte de todos eles. E nós estamos satisfeitos de trabalhar com eles. E para gerar também outro... esta outra estrutura, como para quem quiser mitigar o uso indevido do DNS. Nós pensamos em fazer a nossa parte para podermos enfrentar esse uso indevido crescente, que está no DNS. Muito obrigado pela sua atenção.

GABRIEL ANDREWS:

Obrigado, James. E queria destacar uma coisa. Há uma oportunidade de ação colaborativa. Então, convidamos as diferentes unidades constitutivas, SO e AC do GAC, para que participem, se têm áreas de

ações viáveis, que destaquem as mesmas. Porque sempre há espaço para isso. Muito obrigado.

LAUREEN KAPIN:

Obrigada ao nosso convidado James e Gabe por suas apresentações. Agora, vamos mudar de assunto. Vamos passar a tratar um assunto que já foi tratado, quando o Chris falou dos SSAC 115. E é o tempo para obter as respostas as solicitações de dados do WHOIS. É um tema, que está sendo discutido, estamos debatendo atualmente na equipe de revisão da implementação do trabalho da Fase 1. Eu dou um pouco de contexto. As solicitações urgentes são muito limitadas e se restringem a aquelas circunstâncias, que significam uma ameaça eminente a vida, lesões graves, danos a infraestrutura crítica ou exploração infantil. Nos casos em que a sua divulgação é necessária para lutar contra esta ameaça ou para lidar com elas. Ou seja, é uma categoria muito limitada, muito estreita de solicitações, que geralmente não se formulam. E os representantes do GAC perante a esta equipe, solicitam, que se responda dentro das 24 horas.

E isso se compara com o tempo de resposta de solicitações não-urgentes, que é de 30 dias com base nas recomendações, se contempla especificamente, que o prazo para as solicitações urgentes seja determinado pela equipe de revisão da implementação de trabalhos, que não seja uma coisa determinada pela política.

Isso, queremos destacar para a sua atenção. Porque o que estamos discutindo agora é esta comparação, este período de 24 horas. É uma coisa que para os especialistas na aplicação da lei, às vezes, pode ser

muito extenso, muito amplo. Há um argumento de que se leva realmente até 3 dias úteis, responder essas solicitações. Quando uma coisa acontece dentro de 24 horas uteis ou um dia útil, pode ser que aconteça alguma coisa ruim durante o final de semana seguinte, imediato a essa denúncia. E se concretize, então esse período de 3 dias consecutivos ou úteis, quando surgem no meio de um final de semana. E perante a uma urgência muito urgente, quando há uma ameaça a vida ou lesões físicas ou danos a infraestrutura, esses períodos podem chegar até a 6 dias. Então é uma categoria muito estreita de solicitações, que exige uma resposta muito rápida, para que os organismos de aplicação da lei possam trabalhar e proteger o público.

Seguinte slide. Este tema também está relacionado com os dados de registo. E é uma coisa importante para lutar contra o uso indevido do DNS. E se relaciona com o slide, que apresentou James, quando falou dos atores-chaves, que estão presentes neste ecossistema. Além dos registradores e os registos estão os revendedores. E este tema foi tratado na revisão de CCTs, na recomendação 17. E de alguma forma, encerra esta brecha, que existe quando os registradores publicam os dados e os registos fazem uma solicitação de informações de registo. Às vezes, não é o registor, quem tem a informação, mas uma parte relacionada com o registor, ou seja, um revendedor.

Ou seja, uma recomendação muito simples, que fez a equipe de revisão do CCT, que a ICANN reúna os dados e publique a cadeia de partes responsáveis pelas registões. O Board aceitou esta recomendação e mencionou que já está se colocando em prática. Mas o problema aqui é que embora, às vezes, essa informação está no registo de dados de

registração, não existe a obrigação de que ali, figure. Então, queríamos assinalar este tema, porque continuam exigindo uma ação adicional, para que seja aceita de forma plena. Nós acreditamos que o Board queria dizer ou queria incluir a aceitação plena dessa recomendação. Mas se isso exige a reunião e informação da cadeia de partes, tais como os revendedores, que são responsáveis pela regisração.

A razão pelo qual isto é importante é porque permite os organismos da aplicação da lei, que poupem tempo. Não tem que ir a cada uma das partes, que tenha a informação e em alguns casos, há derivações entre 2 ou 3 partes. Porque podem exigir várias partes envolvidas. Nós achamos que isso é de fácil resolução e esperamos ver algum tipo de medida, que feche, que termine com essa diferença, essa brecha. E ver a possibilidade então, de obter informação para proteger o público através de um problema, de um projeto, de um processo mais simples.

Próximo slide, por favor. Agora, vamos a fazer uma apresentação referida também ao acesso de dados de regisração de nomes de domínio e tem a ver com um estudo recente, em que o Grupo de Trabalho sobre a luta contra o uso indevido de *malware*, mensagens, dispositivos móveis e o Grupo de Trabalho contra *phishing* publicaram há um tempo, atrás se eles vão contar ao respeito na essência, o que aconteceu para... tipo um avanço. E sendo que se trata de um relevamento realizado pelos investigadores na área cibernética e os fornecedores de serviços contra o uso indevido. E essa pesquisa ou enquete tinha como finalidade entender como a aplicação por parte da ICANN, do GDPR da União Europeia, impactou o serviço do WHOIS e o trabalho contra o uso indevido. E discute especificamente a

especificação temporária sobre o acesso por parte dos atores, que trabalham contra o uso indevido e o uso da informação de registo de nomes de domínio, que é essencial e central para diferentes investigações. Nesse sentido, eu então agradeço por ter feito esta atualização.

LAURIN WEISSINGER:

Muito obrigado, Laureen. Eu vejo que os slides já estão na tela. Passamos ao primeiro deles, como falou Laureen, esta é uma pesquisa, uma enquete que fizeram em conjunto, o Grupo de *Phishing* e o MAAWG. Aqui, os atores principais estão aqui, dentro deles, quem fala. **[inaudível – 00:30:32]** e Dave Piscitello, que estão aqui nesse encontro. E vai falar também o Assessor Sênior também.

Seguinte slide. Rapidamente para que todos nessa comunicação saibam o que o MAAWG. Foi criado em 2004. É o Grupo de Trabalho, que luta contra o uso indevido na área de mensagens, *malware* e dispositivos móveis. É o maior da indústria, incorpora todas as partes interessadas, que estão interessadas quanto ao tema corporativo para lutar contra o mau uso de forma corporativa. Por uma parte, nós desenvolvemos e publicamos documentos de melhores práticas, esclarecimento de posição, capacitação, treinamento etc. para ajudar a comunidade em linha a lutar contra o uso indevido. E também fazemos ações de incidência de política pública, das **[inaudível – 00:31:30]** para dar indicações técnicas aos governos e aos organismos de política, para desenvolver políticas e legislação.

Seguinte slide, por favor. Para este estudo, obtivemos 277 respostas. Há diferentes contatos através de listas de correio eletrônico. As respostas foram fornecidas por organismos, que trabalham em cibersegurança, aplicação da lei, segurança pública etc. Mas um grupo, mas sempre como grupo específico, que trabalha ao respeito com estas áreas. Também quero mencionar que os usuários foram muito diversos. Uma coisa que o nosso estudo quer destacar, como se acessam esses registros, que propriedades são necessárias. Por exemplo, alguma grande diferença entre aqueles que utilizam os dados para fazer a análises beta ou aqueles que fazem acessos pouco frequentes ou os organismos da aplicação da lei, para as suas investigações.

GULTEN TEPE: Eu vou pedir ao orador, que fale um pouco mais devagar. Pode ser?

[LAURIN PEDE DESCULPAS E CONTINUA]

LAURIN WEISSINGER: Podemos ver aqui, as pessoas sujeitas a responder a pesquisa. Vemos que a maioria são profissionais de cibersegurança em 40%. Depois em 25% dos profissionais jurídicos e também a comunidade acadêmica, empresas e ISPs e segurança pública. Aqui, estamos comparando um estudo de dados do WHOIS de 2018 e outro realizado ainda este ano. Um estudo que fez o MAAWG também.

Seguinte slide. É importante assinalar, que inclusive, dentro desta amostra tão particular, uma de... tão poucas pessoas participou. Um a cada 10 pessoas fazem que esse... marcam a quantidade de consultas feitas. E vemos que mais de 2 pessoas, vemos que utilizam este uso, desta pesquisa.

Aqui, o que vemos neste slide é que comparando a pesquisa de 2018, que na época, o que estudávamos era o uso combinado. Podemos ver que em termos gerais, vemos uma diminuição quanto ao volume de consultas com pouquíssimos aumentos. E o grupo maior, como aparece aqui, é o dados técnicos, ou seja, elementos que não estão analisados. Em 2021, o nível de consultas é aproximadamente o mesmo. Um pouco mais de 50% das pessoas sujeitas a responder a pesquisa.

Próximo slide. O acesso ao WHOIS está mencionado aqui, nos números que aparecem, em mais de 36% utilizam para fazer consultas na web, consultas do WHOIS com diferentes tecnologias.

Seguinte, por favor. Há muita, mas informações no relatório, que eu convido que vocês leiam. Isto apenas é uma ideia geral. Vamos ver os efeitos da especificação temporária, conforme as pessoas que responderam. Quase 71% dizem que o tempo para mitigar as ameaças supera o limiar aceitável. Esse é um grande problema, ou seja, a especificação temporária tem um efeito especial, quanto a oportunidade. Depois, menos de 10% dizem que as investigações não se veem afetadas. E um pouco mais de 20, dizem que sim, que são

afetadas. Mas que podem continuar trabalhando dentro de um tempo aceitável.

Seguinte, por favor. Se isto, comparamos isso com 2018, vemos que há um leve aumento das pessoas, que dizem que o tempo para mitigar supera o limiar aceitável, de 65 a 70,9%. Um pouquinho pior, digamos.

Seguinte slide. E como podem ver e não deve surpreender, mais de 80% dizem que o tempo para manejar as atividades maliciosas em linha, aumentou e também para manejar os domínios maliciosos. Temos que levar em consideração também, que isso já escutamos várias vezes. Mas vale a pena reiterar. E necessário atuar. As maiorias... a maioria das atividades criminosas, que acontecem é para obter algum tipo de lucro.

Vamos tentar resumir, então estes pontos. Se querem mais detalhes, podem encontrar no relatório. É um tema de interesse, com muito mais gráficos, desenhos e explicações. Apenas ¼ dos pesquisados encontraram fontes de dados alternativos. Atribuição... vê-se prejudicado em grande medida. E não deve surpreender. E aqui, 9 de cada 10 pessoas que respondem, apresentam problemas ou declaram problemas, porque os dados estão sendo expurgados. Mais de 50% consideram, que essa expurgação de dados de pessoas jurídicas e não-europeias é excessivo. E 2,2% consideram que a especificação temporária funciona.

Seguinte, por favor. Então, uma das formas que nós temos para manejar esses dados obtidos é no WHOIS, é enviar uma solicitação para tentar conseguir os dados, que estão ocultos. 34,4% daqueles que responderam, disseram que não o fazem, porque consideram que dá

muito trabalho. Um pouco menos de ¼ efetivamente fazem. E reparem que o resto está dividido entre aqueles, que pensamos que não estavam disponíveis ou que não sabiam como trabalhar com isso e aqueles também que não respondem ou consideram que isso não faz parte da sua realidade.

Seguinte slide, por favor. Aí, vemos novamente que comparado com 2018, os tempos de respostas experimentados pelos que respondem, em termos médios, aumentou. Um ponto que é interessante destacar, esse período de mais 7 dias do qual falamos, uma semana, como média... se comparamos com 2018, houve um aumento de 18%, ou seja, é um longo tempo de espera para esperar os resultados. Isto é aceitável para os dados expurgados? Bem, como podem ver, em geral, a resposta é não. Os pesquisadores... 50% consideram que está bem nas áreas de marcas comerciais e propriedade intelectual para um pouco mais de ¼ está bem. Mas para os outros, precisam de períodos de resposta mais rápidos. *Spam*, 10%. Mas, em geral, não é considerado aceitável pelos entrevistados. Propriedade intelectual. São pessoas que, por enquanto, estariam de acordo.

E próximo slide. E aqui, é onde vemos o que poderia ser considerado como aceitável, por parte dos entrevistados. Vemos que para *malware*, *phishing*, *botnet etc.*, temos uma média inferior a base do marco. Para *spam*, por exemplo, quase 4. Em média, as pessoas estariam conforme com 5.5, os investigadores com 10.

Próximo slide. Com a divulgação aqui, o que queremos é garantir que as respostas sejam, aquelas que são informadas, sejam claras. Mas não

são... são dispares. Às vezes, é recebida um recebimento de aviso. Às vezes, há avisos incorretos.

Também avaliamos o sistema de divulgação, que a ICANN está considerando. Vejam que esses dados são de uns meses atrás. Então provavelmente, se tenham que atualizar-se. Fala de um sistema pago. E é um percentual alto, que disse que não tem os recursos para pagar um sistema dessa natureza. 39% indicaram que sim, estavam dispostos a pagar uma taxa. 78% pagariam uma taxa razoável, 61% aceitariam um sistema por níveis ou preço por volume. A maior parte dos entrevistados disse que um sistema sim, é... não é apropriado pagar por essa informação.

Próximo slide. E por último, embora não seja menos importante, as reclamações perante a ICANN, quão satisfeitos se sentem, quando se apresentou uma reclamação perante o complemento da ICANN, com o manejo que se fez uma reclamação sobre a solicitação de dados de registro. Vemos que a situação não é muito positiva. 45% estão muito insatisfeitos, 35,9% disseram que estão pouco insatisfeitos. E com isso, gostaria de passar a palavra para Bill Wilson, que vai apresentar um resumo da apresentação. Próximo slide, por favor.

BILL WILSON:

Oi a todos. Espero que todos estejam ouvindo bem. Há 4 observações, que acho que podemos tirar de tudo isso. Uma é que todos estamos de acordo em que precisamos de todos os dados relativos possíveis e continuamos protegendo a privacidade das pessoas naturais. Deveriam estar a resguardo. O que se está debatendo na ICANN, dizem

que não vai cumprir com a necessidade das autoridades ou atores no âmbito da cibersegurança.

O terceiro é que nós dissemos que a ICANN deveria estabelecer um sistema funcional, que permita que dados dos registratários possam ser acessados pelas partes credenciadas. É necessário que exista um sistema, tanto para os profissionais da cibersegurança, quanto para autoridades encarregadas da aplicação da lei. Mas tem que funcionar de uma maneira, que elimine parte dessas demoras no tempo. E obviamente, também tem que incluir controles rigorosos de privacidade, de segurança. Tem que haver algum método para prestar contas a esse respeito.

O quarto ponto diz que, como foi mencionado antes, há dois tipos de usuários. Aqueles que usam muitíssimo e outros que são os que usam uma vez, de vez em quando ou com um volume muito inferior. O sistema deve ser capaz então, de gerenciar ambos os tipos de abusadores. Seguente slide. Então como resumo, os 3 pontos, que estão aqui, resumidos. São o que a especificação temporária para o sistema de acesso mostrou que aumenta a quantidade de tempo, como para abordar todas essas coisas e a oportunidade do acesso. É um desafio, realmente, para uma grande quantidade de pessoas. Há outra é que o sistema não é uniforme dentro de todos os registros. Então, quando obtemos certa informação, de determinada maneira de um; mas não dos outros. Então isso gera outro tipo de dificuldades. Tem que existir um sistema de pedidos formais para poder acessar aos dados apropriados em comparação com os outros. Porque em realidade, isso fracassa, porque são rejeitados, ignorados, leva muito tempo s

resposta. Então o que acontece é que demora tanto a resposta, que carece de valor.

E o outro, que são os processos de cumprimento contratual da ICANN, foram descritos como muito longos, ineficientes e que com frequência não fornecem uma solução ou recurso. Esperamos então que possamos modificar essa situação no futuro. Se tiverem alguma pergunta por fora do que esse formulário agora, pedimos que nos enviem um e-mail ao endereço, que está na tela, para poder responder com maior velocidade da qual estivemos falando nessa conversa. Obrigado.

LAUREEN KAPIN:

Obrigada, Bill. Obrigada, Laurin, por essa apresentação tão interessante com exemplos bem concretos da vida real, alguns dos desafios que experimentam os profissionais da cibersegurança, bem como as autoridades da lei. Isso realmente permite continuar pensando os desafios, que temos pela frente, como trabalhar e equilibrar de forma adequada o tema de dados bem protegidos. Mas também, prestar atenção ao que é a segurança pública.

Vamos agora mudar completamente de tema, de assunto. Nesse caso, o nosso colega do Japão, Shinya Tahata vai fazer uma apresentação. Então, vou passar a palavra.

SHINYA TAHATA:

Obrigado, Laureen. Oi a todos! Em primeiro lugar, quero agradecer realmente os copresidentes do PSWG por me oferecer essa

oportunidade de falar. Hoje, tenho umas atualizações, porque houve uma proposta realizada em março, na ICANN70. Então, queria apresentar informação junto com essas ideias. Ao mesmo tempo, que podemos falar em medidas concretas para fortalecer o tema contratual. Na ICANN70, nós chegamos a um entendimento de que havia alguns casos, que tinham conflito com o RAA. Por exemplo, que não se exigia a informação desses registratários e que era desnecessário, que esses registratários tinham que saber quais os dados exatos, que estavam no WHOIS.

Como foi mencionado, o uso indevido dos domínios tinham a ver com alguns registros e registratários. Não com todos. E segundo o grupo de estudos, houve 15 nomes de domínios maliciosos registrados por um único registratário e não seguiam com as disposições do RAA, pedindo a informação dos registratários. Então se é garantido o cumprimento e há empresas que não cumprem, pode ser uma das medidas eficazes contra o uso indevido do DNS.

Quero falar em 3 pontos, que tem a ver com o cumprimento do RAA. Temos que coletar informação certa dos registratários, quando fazem o registro do domínio. Conforme é colocado pelo RAA, os registradores devem coletar a informação dos registratários, como o endereço postal, também o código... o número de código postal. Também tem a ver com as normas da ICANN. E há alguns que não seguem. É por isso, que não podemos diminuir esse uso indevido. Tem que haver auditorias por parte do cumprimento contratual para verificar que isso se cumpre.

Segundo diz o RAA, esses registratários têm que cumprir com certas medidas. E se não o fizerem, podemos ter a suspensão do número de domínio por uma quantidade de dias. E verificar também, que os dados sejam corretos. Portanto, pode se suspender o nome de domínio aos registratários, com base nessa disposição. Também tem que ter a verificação do número de telefone, para verificar a identidade.

Em terceiro lugar, tem que haver uma resposta rigorosa ao que são os relatórios de uso indevido por parte do cumprimento contratual da ICANN. Tem que haver um programa de cumprimento do registratário e é importante pedir provas para demonstrar que esses nomes de domínios não são abusivos. Também devemos ver como se gerenciam esses temas do uso indevido. Isso é muito importante. E tem que haver normas específicas, bem como estabelecer normas para mitigar o uso indevido e que se baseiem no contrato do RAA.

Além desses 3 pontos, podemos falar das listas e da eficácia no futuro, para que os registros e registradores tomem as medidas adequadas. É essencial que os registradores respondam esse uso indevido, verifiquem a identidade dos registratários com base no RAA. Isso serve para garantir o uso da internet. Então, podemos continuar falando nessas reuniões da ICANN sobre os temas, que tem a ver com o uso indevido do DNS e que são de extrema importância para todos os usuários da internet. Muito obrigado pela atenção de todos.

LAUREEN KAPIN:

Muito obrigada, porque em sua apresentação deu propostas muito precisas. Obrigada. Então, temos diferentes sabores dentro do nosso

cardápio de uso indevido do DNS. Brevemente, eu vou falar dos próximos passos, coisa que podem ser possíveis. E depois, vou deixar um tempo para perguntas. Eu sei que esse slide tem a ver com disposições contratuais específicas, para além do tema geral. Mas isso é algo que armou nosso colega do Japão e é muito útil para ter a qualquer momento.

No que diz respeito aos passos futuros, houve muitas propostas que tinham a ver como mitigar o uso indevido do DNS e o uso indevido do DNS em si próprio. O processo de desenvolvimento de políticas de procedimento subsequentes é um grupo específico da GNSO, indicaram que o uso indevido do DNS deve se fazer valer a respeito de todos os gTLDs e não só dos novos gTLDs. É algo que devemos manejar de maneira holística, não só vinculado com a nova rodada de novos gTLDs. E é algo que devemos considerar, é que na primeira rodada de gTLDs, de fato, isso como uma oportunidade, um incentivo para levantar o limiar e fazer com que as disposições contratuais fossem mais poderosas para evitar o uso indevido. Então os contratos para esses novos gTLDs incluem esse uso indevido dos novos gTLDs. Isso foi um avanço positivo. Podemos ter algo similar, inclusive um elemento melhorado para essa nova rodada de novos gTLDs. Porque, de fato, aprendemos da experiência, para os contratos do programa de novos gTLDs.

Embora sejam mais sólidos, continua havendo alguns *gaps* dos quais falamos nas reuniões anteriores, que podemos enfrentar e solucionar na nova rodada, para quando... por isso é que nós mencionamos como um próximo passo, para além de... que sei que existe um debate, uma

discussão sobre esse tema. E sabemos que a perfeição é inimiga do bom. Temos então que tratar ou tentar melhorar. Temos que fazer o que podemos fazer no momento, em que podemos fazê-lo, para poder enfrentar esse problema. Mas cedo do que tarde. Devemos continuar discutindo sobre o uso indevido do DNS.

Qual é a definição? Nós escutamos que há muito desacordo ao respeito. Mas também, de fato, o GAC fez uma declaração bem concreta em setembro de 2019 sobre o uso indevido do DNS. E fez bastante ênfase sobre isso, a um texto que tem a ver com os gTLDs anteriores e trabalho da comunidade anterior, a esse respeito. Também foi indicado para os nossos colegas de toda a comunidade de partes interessadas. Cada um propôs uma definição. E houve esforços voluntários, muito importantes a esse respeito. E isso tem aspectos comuns, que devemos considerar.

Próximo slide. Eu queria fazer referência. Eu sei que deve haver mais tempo para perguntas. Mas queria fazer referências, diferentes definições que existem do uso indevido do DNS. Que também estão mencionadas no trabalho, que eu disse do GAC. A equipe de revisão do CCT preparou a definição que dizia, que eram atividade não-solicitadas, em conivências ou enganosas; que fazem o uso ativo do DNS ou desses procedimentos utilizados para registrar nomes de domínio. E um uso indevido, esse faz referência a outros atos maliciosos. E também temos os contratos da ICANN, que também é amplo, porque falam em proibições generalizadas sobre distribuir os *botnets*, que estão aí sempre ativos; *phishing*. Então, utilizando essas

definições também nos oferece um campo bastante amplo para poder mitigar essas condutas abusivas.

Eu queria lembrar a vocês o fato de que nós sim, contamos com definições sobre as quais podemos nos basear e que obviamente, podemos continuar trabalhando para o futuro sobre esses problemas. Mas temos um alicerce sólido. Analisando os próximos passos, estamos incentivando o GAC a que, quando está trabalhando a comunidade toda, quanto a definição disso ou de uso indevido do DNS e melhorar as disposições contratuais e fazer educação pública. Como mencionamos já, tanto aqui, como em outras reuniões, há uma coisa que nos associam ao ALAC e ter que falar dessa educação. De ter que falar com todo mundo, porque se identificamos, podemos mencionar e depois evitar o problema. Então é muito importante trabalhar sobre este último aspecto. Eu acho que o GAC também pode unir forças com outros membros da comunidade para trabalhar sobre esses pontos. Eu vou pedir a Manal, se talvez, podemos ter 5 minutos para as perguntas ou caso contrário, talvez podemos deixar essas perguntas para outra sessão com, talvez, mais tempo. Mas eu sei que queremos fazer muitas coisas em pouco tempo, que é o que temos disponível. Passo a palavra então, a Manal. E a senhora decide o que fazer.

MANAL ISMAIL, PRESIDENTE DO GAC: Eu entendo, entendo. São muitas coisas, as que temos que tratar nesta sessão. vamos continuar, então com as perguntas. Eu sei que a ideia é revisar rapidamente o Comunicado, na meia hora que temos. Mas podemos, pelo menos, de reprogramar para amanhã. Porque há

outra oportunidade no dia de amanhã para... eu acho que sobre o WHOIS e o EPDP. Temos tempo amanhã. E isso vai permitir fazer algumas perguntas agora. Eu vejo muitas perguntas no chat. Mas também vejo que a mão de Olivier está levantada. Então, passo a palavra a Olivier. E aqueles que querem fazer perguntas, podem fazer de forma oral, claro. Agora, passo a palavra então, ao Olivier.

COMISSÃO EUROPEIA:

Em primeiro lugar, eu quero parabenizar o trabalho do PSWG, porque realmente, nesta sessão, conseguimos apreciar o trabalho feito por esse grupo. Eu acho que esse é um tema muito importante, o que tem a ver com o uso indevido do DNS. E também eu quero apoiar as propostas realizadas por Shinya do Japão. Eu acho que, em definitiva, muitas... ou muitos dos problemas que estamos avaliando ou tratando aqui, podem se solucionar através do cumprimento das obrigações contratuais, fazendo valer essas obrigações contratuais ou exigindo o cumprimento delas. Como já se falou em vários relatórios. Nós tentamos de melhorar essas disposições. Mas eu acho que hoje em dia, o cumprimento estrito dessas disposições são ferramentas, que nos permitem, como dizia Shinya, permitem enfrentar os criminosos. Muitas das partes contratuais cumprem com estas obrigações. Mas há alguns apenas que não. Então, precisamos concentrar nossos esforços neles e solucionar esses problemas.

E também o que tem a ver com a exatidão dos dados de registo. Essa é outra parte muito importante, quando estamos falando do uso indevido do DNS. Fiquei muito interessado no relatório da Laurin. Eu

gostaria de confirmar os dados, do acesso aos dados de registo. Porque é uma coisa muito importante para as autoridades. Há vários especialistas em leis, a França esteve também tentando de promover esse tema dentro do GAC. Quanto ao relatório do SSAC, o SSAC 115, realmente as recomendações que inclui são muito úteis. Oferecem mais apoio, principalmente ao nosso **[inaudível – 01:04:08]** para o nosso debate, que vamos ter amanhã com o Board, para ver como é que vão continuar os próximos passos desse relatório. Obrigado, Manal.

MANAL ISMAIL, PRESIDENTE DO GAC: Obrigado, Olivier. Eu vejo também muitos comentários no chat.

Obrigado, diz aqui o... PSWG, pelos esforços incansáveis de voltar sobre esse assunto com o GAC. Há um comentário também da Índia no chat, que diz: “A educação e o usuário final sobre o uso indevido do DNS e exatidão dos dados do WHOIS vão ajudar a mitigar o uso indevido do DNS. A falta de consciência sobre o uso indevido do DNS nos usuários de internet deve ser enfrentada pelo conteúdo em diferentes idiomas. E para trabalhar, deve-se formar um grupo, que trabalhe sobre os conteúdos do curso. E também, os países interessados deveriam participar no desenvolvimento desses cursos nos idiomas regionais”.

Vejo que também se faz referência e se incluir diferentes links no chat sobre diferentes materiais, que estão sendo disponibilizados. Eu acho que vamos falar também desse tema com o ALAC, quando... da reunião bilateral. Eu vou parar por aqui. E o que eu quero fazer é ver se alguém dos palestrantes têm alguma coisa a acrescentar.

LAUREEN KAPIN:

Eu acho que há um interesse real do ALAC e também do Grupo de Trabalho de Segurança Pública de trabalhar de forma conjunta, esses temas. Eu sei também que os nossos colegas das partes contratadas também estão pensando neste tema, desenvolveram algum material. E podemos colocar toda essa energia e conhecimento. E eu acho então, que então vai valer a pena. A ideia seria que esse material seja traduzido a vários idiomas, para que o público possa se beneficiar deles... desse tema e dos conhecimentos. É uma boa oportunidade, eu acho.

MANAL ISMAIL, PRESIDENTE DO GAC: Agora. Muito obrigada. Muito obrigada, Laureen. Eu não vejo outras mãos pedindo a palavra. Então, se não há mais perguntas, espero não ter perdido nenhuma. Se assim for, que levantem a mão ou que escrevam no chat. Vejo sim, uma pergunta da Dinamarca, que diz “Como a organização da ICANN está tomando a posição de que não é a responsável, corresponsável dos dados? E não podem fazer valer alguns dos requisitos específicos, como pode, cumprimento contratual da ICANN cumprir com a proposta do Japão?”.

LAUREEN KAPIN:

É difícil responder essa pergunta. Eu acho que há certas posições já tomadas com respeito ao papel, a responsabilidade sobre os dados da ICANN e eu me incluo. Acho que não é necessário mencioná-las, mas devemos refletir sobre esses temas. Quero esclarecer que a questão da

exatidão e dados são importantes e que o fato de que o WHOIS seja, se aproprie da responsabilidade sobre este assunto, é importante a disposição do contrato é necessário, que tenha responsabilidades diretas sobre essa composição. E um cumprimento forte das disposições que existem seria muito benéfico. Mas há um trabalho pendente pela frente, como todos sabemos. Existem essas disposições contratuais, mas, no entanto, há um problema de exatidão. Por isso, precisamente, se mencionou a necessidade de trabalharmos a futuro. Já falou a GNSO e este grupo está mais do que disposto a participar desses trabalhos. Esperamos então, chegar a um ponto positivo.

MANAL ISMAIL, PRESIDENTE DO GAC: Obrigada. Passo a palavra para Chris.

CHRIS LEWIS-EVANS: Quero adicionar apenas, mencionar que há uma seção no RAA, que trata sobre os dados do WHOIS, mas algumas disposições do GDPR são um pouco diferentes. Então, como a Laureen destacou, isto exige que continuemos trabalhando na comunidade. Eu sei que o GAC ofereceu a sua ajuda para o trabalho da GNSO.

MANAL ISMAIL, PRESIDENTE DO GAC: Obrigada, Chris. Sim, precisamente, seria muito bom e necessário pensar que a pergunta foi difícil de responder. E a proposta do Japão, que permite incorporar uma pergunta própria. Existe experiência para demonstrar que os nomes de domínio não são abusivos. Eu acho que isso foi justamente um dos pontos apresentados na apresentação.

Então, se aqui, há a experiência de melhores práticas, seria muito útil compartilhá-las. Enquanto isso, continuo com as outras perguntas.

Vejo aqui uma pergunta de **[inaudível – 01:10:12]**, que diz que Lauren fez referência a uma definição proposta pelo GAC, de uso indevido do DNS. Eu acho, Lauren, que a senhora já falou ao respeito.

CHRIS LEWIS-EVANS: Desculpe, Manal. Lauren fez referência a declaração do GAC sobre o uso indevido do DNS. E coloquei aqui, uma cópia do vínculo, do link no chat.

MANAL ISMAIL, PRESIDENTE DO GAC: Sim, muito bem. Agradeço. Vi outra pergunta da Susan Payne. Lauren, de que forma, em posição de novas obrigações sobre os TLDs, que não existem ainda, vão ter impacto naquelas coisas que já estão? Então essas partes, devemos lembrar que em volume, a ampla maioria do uso indevido acontece nos TLDs herdados. Então, por que não se aplicam aqui, esse centro de atenção?

LAUREEN KAPIN: São pontos válidos. A observação de que o grande volume do uso indevido - e é exato isso - acontece nos TLDs herdados. Eu sei. E depende do tamanho e não da proporção. Aí, a resposta a essa pergunta e digo, que essas observações são muito válidas, fazemos o que podemos e quando podemos. Os contratos com os TLDs herdados agora, não estão sendo negociados. Temos esta oportunidade com os

novos gTLDs, porque não têm contratos ainda. Está por ser desenvolvida ainda. Então é a oportunidade de melhorar essas disposições.

Agora, isto vai ter um efeito de cascata sobre os TLDs da primeira rodada? Será? Ou com contrato .COM, e devo manifestar que foram adotadas algumas medidas de proteção no contrato com .COM. Então, eu diria que sim, que existe essa possibilidade de chegar a um impacto possível ou positivo. Mas temos que tomar as oportunidades, que se apresentam.

Eu adoraria realmente, adoraria que estas disposições contra o uso indevido do DNS, acontecessem para todos os TLDs. Mas temos que ser realistas e aproveitar as oportunidades, que surgem. E às vezes, o trabalho que está sempre aumentando, faz com que o efeito seja um pouco de cascata, né? E esse efeito, na minha expectativa, é que consiga melhorar a situação atual. E isso chega através da nova rodada de novos gTLDs.

MANAL ISMAIL, PRESIDENTE DO GAC: Obrigada, Laureen. E desculpem, se esqueci alguma pergunta ou pulei alguma pergunta. Espero... ver se há mais perguntas. Mas eu quero agradecer de todas as formas, então o link ao chat. É muito interessante e informativo também. queria saber se há alguma pergunta sobre soluções possíveis a respeito deste tema. Aqueles que manifestaram a sua insatisfação, eu pergunto se também apresentaram alguma solução possível?

LAURIN WEISSINGER: Muito obrigada. Está por chegar o MAAWG com a colaboração do PSWG e vai trabalhar na análise de soluções possíveis, incluindo outras partes interessadas. Então teremos que voltar com essa resposta no final deste ano, com um segundo documento. Reunimos os dados, como primeira etapa. Depois veremos a política, faremos alguma observação do que dizem os dados. E as perguntas oferecem alguma informação. Mas o relatório das perguntas é uma coisa diferente de encontrar soluções. Temos que analisar. Esperemos poder apresentar esse trabalho no final deste ano.

MANAL ISMAIL, PRESIDENTE DO GAC: Obrigada, Laurin e outros apresentadores do PSWG, a do Japão. Também do MAAWG.

Uma sessão muito informativa. E com isso, então termina a nossa Sessão de Discussão de Medidas de Mitigação do Uso Indevido. Pedimos aos membros do GAC, que permaneçam na sala, porque vamos aproveitar estes minutos que temos, para fazer uma revisão muito rápida do Comunicado, da redação do Comunicado. Muito obrigada a todos. E por favor, me informem, quando podemos começar com esta rápida análise do Comunicado.

[FIM DA TRANSCRIÇÃO]