ICANN78 | Assembleia Geral Anual – Discussão do GAC sobre abusos do DNS
Quarta-feira, 25 de outubro de 2023 – 10h30 às 12h HAM

GULTEN TEPE: Olá e bem-vindos a Discussão sobre o Abuso do DNS do GAC na ICANN78 em 25 de outubro, às 10h30, hora local. Eu sou Gulten Tepe. E sou a gerente de participação remota desta sessão. Esta sessão está sendo gravada e é regida pelas Normas de Comportamento da ICANN.

As perguntas e comentários só serão lidos se estiverem no formato correto. Teremos interpretação nos seis idiomas da ONU e português. Cliquem no ícone de interpretação do Zoom e selecionem o idioma, em que vão ouvir durante a sessão. Se quiserem falar, levante a mão no Zoom. E quando o facilitador chamar o seu nome, ativem o microfone.

Antes de falar, veja se selecionou o idioma, em que vai falar no menu de interpretação. Diga o seu nome e o idioma, que vai falar, se não for o inglês. Ao falar, silencie todos os dispositivos e notificações. Falem claro para uma boa interpretação.

Para ver a transcrição em tempo real, clique no botão de *Closed Caption* no Zoom. Para garantir a transparência de participação no modelo multissetorial da ICANN, inscreva-se no Zoom, usando seu nome completo. Com isso, eu passo a palavra ao presidente do GAC, Nicolas Caballero.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Bem-vindos. Teremos uma sessão de 90 minutos sobre o Abuso do DNS, que é um tema muito sensível e importante para o GAC. Temos uma equipe fantástica de oradores convidados. E eu vou deixar que se apresentem, começando com o Graeme.

GRAEME BUNTON: Eu sou diretor executivo do Instituto do Abuso do DNS.

LAUREEN KAPIN: Olá. Eu sou Laureen Kapin, falando como uma das copresidentes do Grupo de Trabalho de Segurança Pública.

NICK WENBAN-SMITH: Eu sou Nick Wenban-Smith. Eu estou falando aqui, como presidente do Comitê Permanente de Abuso do DNS da ccNSO.

SUSAN CHALMERS: Eu sou Susan Chalmers e eu trabalho para o Ministério, o Departamento de Comercio. E eu sou representante dos Estados Unidos no GAC.

CHRISLEWES-EVANS: Olá! Chris Lewis-Evans. Sou diretor de Relacionamento com os Governos e a Mitigação do Abuso, CleanDNS.

SAMANEH TAJALIZADEHKHOOB: Eu sou a Samaneh. Eu sou do Escritório da ICANN da CTO.

NICOLAS CABALLERO, PRESIDENTE DO GAC: E com isso, eu passo a palavra imediatamente a Laureen Kapin, que vai falar... perdão, Susan Chalmers. Desculpem. Susan, pode falar.

SUSAN CHALMERS: Nós temos uma agenda bem apertada. Eu vou falar sobre os antecedentes do Abuso do DNS; as emendas ao contrato, que estão em Período de Votação. Depois vou falar do Comentário Público do GAC durante esse Período de Comentários Públicos sobre as emendas.

Ao redor de 2019, o GAC começou a discutir o Abuso do DNS, falando com outras partes da ICANN. As partes contratadas responderam com uma proposta proativa de tratar o Abuso do DNS no final de 2022. A proposta de negociar novas obrigações de Abuso do DNS nos seus contratos e o nome desses contratos estão aqui, no slide.

Em maio de 2023, a minuta das emendas foi publicada. Começou o Período de Comentários Públicos em julho de 2023. O GAC fez um comentário público. Em outubro, o Período de Votação para adotar essas emendas foi aberto. E deve ser fechado em dezembro.

Antes da ICANN77, alguns membros do GAC devem lembrar, nós, no Grupo de Regiões Subatendidas, fizemos dois webinars para dar fundamentação ao Abuso do DNS e sobre as emendas. E eu convido vocês a olharem esses webinars no site do GAC. Depois disso, na ICANN77, tivemos uma Oficina de Capacitação, organizada pelo Grupo de Trabalho de Regiões Subatendidas, junto com os Estados Unidos. O enfoque foi sobre as emendas aos contratos, quanto ao Abuso do DNS

e como o GAC pode trabalhar para fazer um comentário durante esse Período dos Comentários Públicos.

Vários voluntários participaram durante esse prazo muito curto para elaborar um comentário público. E esses representantes do GAC foram da China, Taipei, Colômbia, Egito, Comissão Europeia, Mali, Suíça, Reino Unido, Estados Unidos. Nós fizemos uma consulta ampla com todos os membros do GAC. E esse comentário também foi fundamentado pelo Grupo de Trabalho de Segurança Pública.

Então houve apoio geral a emenda. E eu gostaria que vocês lembrassem o que é incentivar registros e registradores de cada uma das nossas regiões para haja adoção dessas emendas. Lembre disso. E o Período de Comentário Público também tratou áreas de futuro trabalho. Passo a Laureen Kapin.

LAUREEN KAPIN: Bom, então eu espero que falando isso, se torne realidade. Quando as emendas do contrato forem aprovadas, ainda há trabalho a ser feito. E isso foi discutido no comentário do GAC nesse tema. Uma das áreas discutidas foram processos de elaboração de políticas, direcionados para informar esses contratos. Quando eu falo em direcionados, eu quero dizer que a ideia é que o trabalho seja feito mais rapidamente.

E eu gostaria de lembrar aqui e também para estimular a discussão de como fazer com que isso se torne viável. E então, orientação sobre termos-chave, como adequado, imediato, acionável, razoável referindo-se ao tipo de provas, respostas. Uma ideia é que poderia haver o estabelecimento de indicador ou elementos de dados do que

seria uma prova acionável e quais seriam as ações adequadas de mitigação.

Outro problema e eu repito aqui, um problema é como tratar o abuso persistente. Então as atividades do abuso do DNS, como isso é rastreado. E a Equipe do CCT e do SSR2 tiveram boas ideias sobre esse tema. E esse trabalho foi realizado por várias pessoas de diferentes grupos.

Também a ideia de quais incentivos podem ser criados para os registradores, que têm resultados positivos no tratamento do abuso. Podem ser financeiros ou não. Então a afirmação também dessa atividade de forma pública, que seriam formas não-financeiras incentivar um bom comportamento. Se os registrantes acham que foram suspensos sem justificativa, qual é o processo de apelação? E finalmente, o treinamento que sempre é bom, o treinamento sobre a prevenção e a mitigação do Abuso do DNS, para que os atores atuais e futuros desse ecossistema possam promover o bom comportamento e manter o espaço seguro.

Há outras áreas para trabalhos futuros. E isso deveria ser feito idealmente antes da próxima rodada. Uma das coisas são as consequências as emendas, não incluem expressamente as consequências, então o que acontece se não há conformidade. Seria muito produtivo para a ICANN Org e as partes contratadas, quais são as consequências, se as obrigações não são cumpridas. A capacidade de monitorar a aplicação é essencial, seria muito útil que houvesse transparência sobre os resultados dessas emendas. E esse poderia ser um tema de futuro trabalho.

E finalmente, a evolução do Abuso do DNS. E a Equipe do SSAC escreveu isso na publicação SAC115. Então esse abuso se envolve, sempre se encontram novas formas de escapar a essas restrições. E nós temos também que fazer isso. Nenhuma definição deve ser estática. E esse pode ser um tema de análise de todas as partes da comunidade, como cibersegurança, pesquisa acadêmica ou independente, cibersegurança etc. E essa pode ser uma área muito produtiva de futuros trabalhos.

Nós sabemos que a recomendação foi publicada sobre as emendas. Esse documento deve ser um documento vivo. Porque o cenário pode mudar e esse documento deve mudar de acordo. São alguns dos tópicos identificado no comentário do GAC e devem inspirar o nosso trabalho futuro.

SUSAN CHALMERS: Muito obrigado, Laureen. Gostaríamos de abrir agora para a discussão. Teremos 10 minutos para isso. E depois passaremos para as apresentações dos convidados. E teremos mais um tempo para discussão antes do encerramento. Então se houver alguma pergunta, comentários.

GULTEN TEPE: Temos aqui inscritos Índia, China e Japão.

SUSHIL PAL: É uma pergunta sobre o comercio eletrônico. Então nós vemos isso já, todos os dias. Por que seria um trabalho futuro? Por que não agora, trabalhar nisso agora?

SUSAN CHALMERS: Obrigada por sua intervenção. Esse é um tema de discussão em andamento no GAC. Eu acho que temos sessões de Abuso do DNS já há 7 anos no GAC.

SUSHIL PAL: Então o que este listado em futuro trabalho, então são atividades que foram realizadas antes. Então o que eu acho importante é ver isso em relação aos contratos. Apesar das medidas de mitigação aplicadas, ainda estamos abandonados por assim dizer. E nós não podemos fazer nada, só entrar em desespero. Então eu acho que a gente deveria... eu sei que vocês já devem ter discutido isso há muito tempo. É... a primeira coisa é discutir esses contratos. A nossa ação não está mantendo o mesmo ritmo, que o cibercrime. Então nós estamos sofrendo *hacking* o tempo todo. Como é que nós monitoramos isso? Como conter isso?

SUSAN CHALMERS: Eu concordo com você. É uma questão de prioridade. Por isso é tão importante incentivar os registradores nas nossas jurisdições a votar a favor das emendas. E eu acho que em San Juan poderemos discutir mais sobre isso.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Eu concordo, não como Presidente do GAC, mas a título pessoal. China, Japão e Colômbia. China.

WANG LANG: Muito obrigado. Sou Wang Lang da China. A ICANN abriu um Período de Votação para as emendas propostas. E há dois limiares para aprovação do RAA. Então a aprovação pelos registradores de 90% dos registros de nomes de domínio de registração. E para os registradores, a aprovação de 2/3 dos registros. A minha pergunta é: "Como esses limiares foram estabelecidos? E a perspectiva é otimista?".

SUSAN CHALMERS: Sim. Há um link para rastrear isso, fornecido pela ICANN, para informar-se em tempo real. Fabien vai publicá-lo aqui no chat para seguir, acompanhar os progressos.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Sim, agora é a vez do Japão.

NISHIGATA NOBUHISA: Bom dia. Fala Nobu Nishigata do Japão. Primeiro, obrigado pela apresentação, pelo trabalho feito. Eu tenho algumas perguntas. E a primeira é sobre os termos-chave e também esses apropriado, imediato, viável e razoável.

Esses termos já existem no texto do RAA no ponto 18. E poderíamos ter algum tipo de orientação sobre isso. E essas seriam as ações... poderiam ser aplicadas ao... esse texto, considerando que são os mesmos termos.

Depois a evolução do DNS. No final da apresentação, eu me pergunto se algum colega tem ideia sobre como incluir na discussão futura,

algum tipo de Abuso do DNS. Não tenho muita certeza, mas a expansão do cenário atual, requer isso.

Quanto ao que o colega da Índia mencionou, eu concordo com ele, com o que o Nico também mencionou. Não só o Abuso do DNS, mas também alguns comportamentos maliciosos na internet. E seria bom termos alguma... estabelecer alguma relação entre o GAC e aqueles que controlam os ccTLDs. Não estou falando na ccNSO, mas essa é um problema compartilhado pelos governos. Portanto acho que deveríamos perguntar-nos mais sobre esse assunto, para continuar com a discussão no futuro.

SUSAN CHALMERS: Eu vou responder brevemente a primeira pergunta, Nobu. Essa primeira pergunta, esses termos foram expandidos numa recomendação, mas ainda temos questões abertas a respeito disso, que devem ser definidas com a comunidade.

LAUREEN KAPIN: Sim. Eu gostaria de agregar aqui ao que a Susan disse. Aqui se temos PDPs direcionadas sobre essa ação, esse entraria no âmbito dos PDPs para definir como isso vai ser incluído e acionado nos contratos. Os mesmos termos também, temos flexibilidade, sim. Isso vai depender do futuro trabalho sobre políticas.

Também algo que não foi mencionado aqui, é que isso deve ser feito dentro da ICANN e fora da ICANN. Ouvi aqui o Japão, a Índia falando sobre as dificuldades com essas questões são difíceis em diferentes

países, especialmente, quando há problemas que envolvem vários países, além das fronteiras. E deve haver algum tipo de cooperação, de acordos de cooperação, de compartilhamento de informações. Isso fica fora da ICANN, mas é um trabalho muito importante para permitir que as forças da lei ou organizações de consulta do mundo cooperem entre si, além das fronteiras.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Obrigado, Laureen. Eu não sei, Japão, se você levantou a mão de novo. Não? Colômbia, então. Representante da Colômbia, não sei se está aqui.

THIAGO DEL-TOE: Sim. Não... eu já não preciso falar. A minha pergunta é a mesma, que a do Canadá.

PEARSE O'DONOHUE: Oi! Pearse O'Donohue. Então uma observação. A Comissão Europeia realmente apoia essas emendas aos contratos. E espero que haja uma votação para alcançar as cotas. E também devemos lembrar que haverá uma consulta pública e com uma resposta.

E tivemos essa consulta com nenhuma resposta, nenhuma proposta. E isso ficou... fora da incumbência do modelo multissetorial. Devemos considerar que há contratos. E temos entre a ICANN Org, parte contratadas e de novo, há necessidade de incluir os setores interessados também nesse processo multissetorial, para opinar e

fazer comentários e dar *input*s diretamente sobre a implementação. E é por isso, que eu...

Quanto ao monitoramento proativo, que não foi assumido, devemos lembrar que o PDP deve ser amplo e abrangente, além de estar direcionado.

NICOLAS CABALLERO, PRESIDENTE DO GAC: É a vez do Canadá.

JASON MERRITT: Obrigado. Jason Merritt. Brevemente, antes de passarmos a um outro assunto, o Canadá apoia as emendas aos contratos. Apreciamos muito... feito pelas partes contratadas da ICANN. Aqueles se reuniram para negociar e encontrar alguma solução tangível. Foi um passo positivo. E teremos mais oportunidades. E realmente, esse é um progresso incremental, que não é automático. É algo ao qual devemos prestar atenção. E é isso que eu queria expressar. Sempre apoiamos e apreciamos esse trabalho da comunidade com as diferentes partes consultadas. É um trabalho enorme, um passo enorme. E somos cientes disso. Portanto agradeço muito.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Pediu a palavra, Irã.

KAVOUSS ARASTEH: Bom dia. Corrijam-me, se eu estiver enganado. O ano passado, houve alguma emenda e continuamos falando emendas. Estamos falando em

emendas futuras e qual é o escopo das futuras emendas neste caso? E qual é o resultado da primeira emenda? E se a ICANN via oferecer algum tipo de informação sobre essa questão?

SUSAN CHALMERS: Obrigada, Kavouss. Essa é a primeira emenda, a primeira iniciativa com emendas. Porque isso tem a ver com o Abuso do DNS. E isso tem a ver com o RDAP. A primeira iniciativa conjunta, então. Obrigada.

LAUREEN KAPIN: Kavouss, houve alguns materiais informativos, preparados. A ICANN Org, no site também tem os antecedentes desse processo das emendas. Ainda não foi concluído. Está em andamento. E esperamos que seja aprovado em dezembro.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Obrigado, Laureen, Susan e Irã. Mais alguma pergunta antes de continuarmos aqui, na sala ou online? Indonésia pediu a palavra.

ASHWIN SASTROSUBROTO: Tivemos um acordo sobre... estamos de acordo sobre o que registradores devem fazer. Mas também há algum tipo de sistema de certificação também para os registradores seguirem a ISO, por exemplo, em questões de segurança, algum tipo de conjunto de padrões a serem seguidos. Obrigado.

SUSAN CHALMERS: Obrigada pela pergunta. Eu não sei se a ISO tem algum tipo de requerimento e procedimento, quanto a segurança. Poderíamos continuar falando sobre isso depois *offline*. Obrigada.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Obrigado, Susan, Indonésia. Mais algum comentário ou pergunta? Então vamos continuar com a nossa agenda. Susan.

SUSAN CHALMERS: Agora vamos as apresentações com o Instituto de Abuso do DNS.

GRAEME BUNTON: Obrigado, Susan. E a todos, eu peço desculpas. Quem fala é o Graeme Bunton. No *workshop* de sábado de capacitação, falamos sobre isso. Eu sou Graeme, eu sou o diretor do Instituto de Abuso do DNS para registros de interesse público, para tentar resolver problemas de Abusos do DNS em todo o setor.

Eu fiz slides ontem à noite. Não consegui aprimorá-los muito. Mas brevemente eu vou falar sobre o Projeto da Bussola, medição de abusos e também medição do impacto das emendas. E isso... bom, vou ser rápido.

E criamos esse projeto chamado de Compass, Bússola para a comunidade da ICANN, que realmente precisa participar dessa elaboração de políticas sobre dados, trabalhando com registradores. E criamos uma abordagem transparente para lidar com os Abusos do DNS. Isso foi ano passado, com relatórios mensais, que foram

publicados e que vocês podem consultar no link. Eu vou colocar o link do Compass. Então relatórios mensais com tendências em toda a indústria. Temos uma espécie de lista, são listas tipo Top 10, que vocês podem consultar.

Aqui, esse é um slide um pouco complicado. É muita informação e esse é um... aqui, medimos os abusos para interessar-se quanto a medição de abusos específicos. Hoje à tarde, a Laureen vai fazer uma apresentação sobre essa questão mais em detalhe.

Agora, aqui o importante é como funciona a medição de abusos. Precisamos ter algum tipo de informação sobre o abuso em questão. É questão que tem a ver com os RBLs, que são listas de bloqueio de reputação. Há problema também, às vezes, com as fontes, nomes de domínio. Essa lista deve ser limpa ou duplicada. E fazemos uma para determinar se são maliciosas ou não, ou se há sites que estão comprometidos também ou prejudicados.

E depois monitoramos o tempo do **[inaudível – 00:35:25]** em tempo real. Quanto dura o *hacking*? 30 dias, 5 minutos, 10 minutos. O que nos permite medir não apenas as taxas de mitigação, mas também o tempo desde a denúncia até a mitigação. E também observamos se algum TLD ou registradores aqui, na sala. Também oferecemos *dashboards* personalizados para a comunidade. São gratuitos. E para os TLDs específicos, os registradores de gTLDs, ccTLDs também; para que saibam, tenham uma ideia de onde se encontram.

Aqui temos as taxas gerais de abusos. Realmente são algumas tendências, se houve alguma mudança em dezembro 2022 e janeiro de

2023. Isso porque um provedor específico de serviços gratuitos saiu do ar. Mas se considerarmos esses dados, do ponto de vista histórico, vamos ver que não houve muita mudança ao longo do tempo.

E quanto as emendas, o impacto que terão. O que eu... acho que por um tempo longo, vamos ver uma diminuição dos abusos, as taxas de abusos. Não vai ser imediato, porém. Mas sim, vai levar um tempo. Também o impacto das emendas. É importante considerar para onde eles vão e se resolvem ou não o ciberdelito. Bom, aqui, a medição das taxas de mitigação, vamos supervisionando essas taxas ao longo do tempo. Também pode ser que o nome tinha sido suspenso pelo registrante, pelo registro. Ou também pode a companhia de *hosting* pode fazer isso. Outra vez o criminoso, talvez tenha desativado aqui, a ação. Mas isso mostra que o dano já não está presente.

Em laranja foi... na cor laranja não foram mitigados, verdes mitigados; o laranja claro, sem categorizar. Então vemos uma mitigação, um prazo de 30 dias. Isso vai aumentar um pouco. Depois as emendas. Espero que seja rápido. E esperamos que essas taxas de mitigação, então aumentem e melhorem.

Então aqui, esses são dados dos *dashboards*, oferecidos aos registradores. O tempo médio de mitigação é... e vemos que há alguma variabilidade. Mas na média são 24 horas. E isso é para dizer que o que vai ser útil aqui, para entender o impacto das emendas, é o que eu vou mostrar agora, que são taxas gerais de abuso, as taxas de mitigação gerais e o tempo médio até obter a mitigação.

Sou otimista. Esse é o meu trabalho, causar impacto. E acho que as taxas de mitigação vão melhorar à medida que o setor for incentivado. Isso vai ser ao longo do tempo. É isso que eu tinha para mencionar aqui. Se estiverem interessados nessa medição de abusos, vejam hoje à tarde, a sessão da ccNSO. Obrigado.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Muito obrigado, Graeme. Há alguma pergunta?

GRAEME BUNTON: Eu queria acrescentar que fazemos isso gratuitamente. Se você é registro ou registrador ou quiser entender melhor o abuso., nós queremos informar a comunidade. Muito obrigado.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Muito obrigado. Bem, como não há perguntas online e na sala, então passamos a Susan Chalmers.

SUSAN CHALMERS: Eu acho que a perspectiva de usar ou medir os efeitos do contrato, eu acho que é muito interessante. É muito importante ter esses dados. Então agora, eu vou passar para a OCTO da ICANN.

SAMANEH TAJALIZADEKHOOB: Obrigada, Susan. Eu sou Samaneh. Sou diretora de Pesquisa em Segurança, Estabilidade e Resiliência no Escritório da ICANN do OCTO.

E eu lidero a Ferramenta de Relatoria. Espero que seja útil essa apresentação.

O DAAR foi lançado em 2017. Então agrega dados de listas de reputação agregados por TLD. Então contagem por TLD com bina, a contagem de domínio de arquivos-raiz, arquivos da zona. E mantém uma conta diária.

E faz então relatórios mensais. Nós temos relatórios. Esses relatórios mensais são publicados na página do DAAR e o acesso diário através da API. Como a ferramenta já está sendo usado há vários anos, nós podemos então elaborar tendências de longo prazo.

Aqui, vemos como funciona de forma simplificada. Então há RBLs e há uma... arquivos da zona, que são combinados, produzindo métricas que são percentagens normalizadas por tamanho de TLDs. Eu tento explicar como a ferramenta funciona, de forma simples. Mas outra vez, que eu apresentei essa ferramenta ao GAC, por falta de tempo, eu não vou poder entrar aqui, em muitos detalhes. Mas vocês podem falar comigo depois.

Aqui, isso é um tipo de gráfico, criado pela ferramenta no relatório mensal. Aqui, vemos a distribuição dos 4 tipos de abusos em gTLDs tradicionais e novos. Então dependendo do tipo de TLD, as ameaças podem ser diferentes. *Malware* há mais nas tradicionais. Enquanto nos novos gTLDs, temos mais *spam*.

Esse é um outro gráfico do relatório. No eixo Y, a percentagem de abusos e no X, vocês veem o tamanho do TLD. Cada círculo é um TLD.

Então vemos quanto maior o círculo no gráfico, mostra a quantidade de abuso nesse TLD.

Isso não está incluído no relatório mensal. No X, temos uma longa linha de tempo. E eu gerei esses gráficos ontem. Nós temos aqui, 5 anos. E é mais ou menos assim, que é o Abuso do DNS desde que começamos a coletar os dados do DNS. Então uma redução de domínios no *command and control*, comando e controle.

Então eu sei que o Projeto DAAR é considerado de diferentes formas dentro da comunidade da ICANN. Mas o fato é que o Projeto DAAR hoje, tem algumas limitações. Há coisas que pode ou não fazer. Atualmente, podemos relatar atividades de ameaça em nível de TLDs. Pode fazer análise histórica dos 4 tipos de abusos coletados. E esses dados como são agregados e anonimizados, não podem ser usados para tomar ações. Mas pode dizer onde estão concentradas as ameaças á segurança.

O que o DAAR não faz no momento, não dá dados em nível de registrador, mas só de registro. E também não tem informações sobre estratégias de mitigação. O sistema não tem mecanismo para diferenciar a domínios registrados maliciosos ou comprometidos.

Então, e agora? Já faz um ano, do Grupo de Segurança, Resiliência e Estabilidade na OCTO. Queremos passar para um próximo nível. Recebemos a análise das Equipes de Revisão e levamos isso em conta. Consultamos várias partes da comunidade. E queremos incorporar isso na próxima plataforma.

Hoje estamos definindo exigências para o projeto. O projeto é interno. É percebido como uma plataforma de medição modular. Vamos agregar módulos e funcionalidades. Como há muitas coisas, que queremos fazer com esse projeto, nossa é muito pequena. O primeiro módulo será métricas para registros e registradores, que estão no sistema DAAR. Haverá um painel de controle ou *dashboard* dinâmico para mostrar gráficos. Haverá uma funcionalidade de busca para diferentes usuários. E os ccTLDs também vão participar. Há uma API pesquisa pela academia.

Então depois do primeiro módulo, são outras coisas que queremos agregar ao projeto. Em geral, não... de início, então depois do primeiro módulo lançado, talvez daqui a um ano, são outras coisa que queremos agregar.

STEVE SHENG: Então listas de reputação, nível de domínio. Então métricas para medir o tempo ativo de forma robusta, para diferenciar tipos de domínios maliciosos ou domínios comprometidos. Queremos a detecção de páginas estacionadas, a predição de abuso.

As pesquisas, os pesquisadores do SSR estão trabalhando. E esperamos a cada ano, agregar módulos ao sistema. Teremos mais informações na sessão do ccTLD esta tarde. Muito obrigada.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Muito obrigado. Há alguma pergunta? Temos a Índia.

T. SANTHOSH: Muito obrigado. Uma ótima apresentação. Eu gostaria de saber, se pode-se mitigar o abuso de domínios maliciosos sobre o DNS, o HTTPS? É muito difícil de diferenciar o tráfego. Se é possível detectar o domínio malicioso via DOHT ou DOT?

SAMANEH TAJALIZADEHKHOOB: Bem, o que você falou é um mecanismo para realizar uma atividade maliciosa. O que a ICANN faz, o que a ICANN Org faz, o DAAR e outros projetos. Nós não fazemos essa detecção. Nós só trabalhamos com domínios, que são denunciados. Nós não fazemos essa detecção. Nós só utilizamos o domínio da lista e investigamos para encontrar prova de abuso.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Índia e agora, China.

WANG LANG: Muito obrigado, Nico. Wang Lang da China. Nós sabemos que há um Comitê sobre o Abuso do DNS. Há um comitê permanente. E também há um pequeno grupo na GNSO sobre o Abuso do DNS. Qual é a diferença entre esses grupos, quanto aos seus resultados, objetivos?

GRAEME BUNTON: Eu... poderia responder isso. Mas eu gostaria que você esperasse até a minha apresentação, onde eu explico isso. Muito obrigado.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Há mais alguma pergunta mais? Bem, desculpa. Índia.

SUSHIL PAL: A ICANN tem algum plano de relacionamento com países, que estão enfrentando múltiplos ciberataques, em termos de capacitação?

SAMANEH TAJALIZADEHKHOOB: Pelo menos pela parte da OCTO. Na Equipe de Relacionamento, talvez você já tenha tido contato com eles. Nós do SSR, estamos trabalhando com o .IN da Índia. E talvez eu posso botar você em contato com a nossa equipe.

GRAEME BUNTON: Eu queria agregar que estivemos recentemente no Vietnã, para fazer então divulgação e capacitação e oferecer melhores práticas, informações a qualquer um, que precise. Então vocês podem entrar em contato conosco nesse serviço, chamado NetBeacon, que é gratuito.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Tajalizadehkhoob é o seu nome mesmo? Mais alguma pergunta? Se não, eu passo a palavra ao Chris.

CHRIS LEWIS-EVANS: Então foi bom falar de novo com o GAC. Eu quase tive síndrome de abstinência, de não participar. Então é um trabalho CleanDNS de relacionamentos com os governos. Trabalhamos com registros e

registradores e provedores de hospedagem. E eu vou mostrar aqui, as informações necessárias, alguns relatórios.

Então o que é um problema, é a falta de relatoria em cada país. Eu acho que o padrão é que encaminhar é muito importante. Então uma ferramenta, como o NetBeacon, é muito importante. Também recebemos informações de listas de abusos. Às vezes, essas listas não são muito coerentes. Então o que é importante é ter múltiplas fontes, para as denúncias de abusos.

Os nossos clientes têm, então diferentes formulários para... às vezes, formulário na web. O que é importante para o lado da cibersegurança, essas fontes têm muitas informações de abuso e também as fontes governamentais. É muito importante.

Eu sei que o Reino Unido tem um formulário para denúncia de e-mails maliciosos, para *phishing*. Então continuando sobre as denúncias no CleanDNS. Nós achamos que precisamos mitigar o máximo possível, o mais rápido possível. Recebemos denúncias de abuso de qualquer fonte, qualquer registro e registrador ou hospedagem. E isso é processado, comprovado. Se houver um problema, nós vamos tratar, se não isso será encaminhado para a parte adequada.

Então, como por exemplo, o NetBeacon que vai encaminhar isso para a parte relevante. O que é muito importante da denúncia e 'ter o *feedback*. Os denunciantes não gostam de fazer uma denúncia e que tudo desapareça no buraco negro, especialmente se você for uma vítima, é importante ver que algo aconteceu. Então nós damos

feedback sobre o que aconteceu nesse domínio. E isso em si é considerado um bom resultado.

E o que falou o Graeme é chave para a mitigação de abusos. E é o tempo, que nos leva a desativar um abuso. Quanto menos tempo, menor a probabilidade de que o *malware* cause prejuízos, menos vítimas. E é muito difícil quantificar os impactos, que o *malware*, *phishing* causam nos nomes de domínio sem denúncias.

Então CleanDNS, nós, o que vemos, são os diferentes tipos de abusos. O e-mail com *phishing* não é a mesma coisa, que o *malware*. E portanto é importante poder qualificar cada um desses dados. Muitos podem ser percebidos e capturados visualmente, mas nem todos eles. O *download* com *malware*... bom, não é fácil de registrar através de uma foto de tela.

Então devemos ter registros de ações, que sejam viáveis e aqui, tem uma lista, listas das coisas que fazemos. Mas a denúncia é fundamental, primeiro. É o primeiro passo. Depois é ter capturas de tela, também tem a informação no cabeçalho, os dados de registro, URLs etc.; são todos dados importante. Também não recomendo que vocês façam o *download* do *malware* para a enviá-lo aqui, a gente. Não.

Então na lista, que eu mencionei, há muito PII, aqui. E quanto as provas, não precisamos provas de PII, nem nas denúncias, as provas de abusos. E é possível que tentemos automatizar isso no menor tempo possível, coletar as informações necessárias e combiná-las para aproveitar no máximo essas provas.

E em geral, não utilizamos PII. E a pessoa mais apropriada agir, poderia ser o registrante com esse tipo de abuso. Precisaríamos de usar um

contato com o registrador ou contato com o registrante, com o provedor de *hosting* e utilizar o WHOIS para colher dados. E bom, fico aqui aberto, para responder perguntas.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Obrigado, Chris. Eu vou abrir aqui, o espeço para perguntas e comentários online e também presenciais.

LAUREEN KAPIN: Rapidamente, eu ouvi e quero destacar que os dois últimos oradores, realmente devemos agradecer muito a eles. Porque foram avisados no último momento, que deviam fazer as suas apresentações. Realmente apreciamos muito o esforço.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Por favor, uma salva de palmas aqui, para todos eles. e eu já tenho duas solicitações para falar. A Índia e o Irã. Índia, por favor.

T. SANTOSH: Basicamente, o SubPro ou o rastreio do SubPro dos novos gTLDs... e também a outra forma de rastreamento no WHOIS. Obtemos comunicações frequentemente do secretariado do GAC. Quanto aos abusos do DNS, devemos então até o site da ICANN para buscar todos os relatórios de denúncias. Ao secretariado do GAC então, solicito que envie um relatório mensal por e-mail com essas informações. Seria muito útil.

KAVOUSS ARASTEH: Obrigado. Sim, eu também aqui, aprecio muito o trabalho. Foi muito rico, muito interessante. E sugiro que vejamos quais são as formas e e-mails para acompanhar as ações, do que está sendo feito. Acompanhar e ver e para depois ter de informar-se sobre resultados em porcentagens. É importante definir como fazer essa tarefa de acompanhamento. Então ontem e hoje falamos de Abusos do DNS, mas devemos pensar também em como informar no futuro.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Obrigado.

CHRIS LEWIS-EVANS: Podemos dar apoio aos registradores e registros. Exceto quando houver mudanças nos contratos e o canal, o Canadá mencionou. Esse é um passo muito importante, que melhora o ataque aos abusos ou as resoluções de abuso. Então excelente passo.

SUSAN CHALMERS: Obrigada, Chris. Sim, Kavouss, sugeriu enviar isso, a lista de e-mails e fazer uma troca de informações, publicar atualizações, especialmente antecipando a reunião da ICANN79 em San Juan. É muito bom colaborarem, mantermos informados.

KAVOUSS ARATEH: Sim, o colega do Canadá mencionou que a questão que tem a ver com os registros e registradores está fora da **[inaudível – 01:07:49]** dos setores interessados. Como é que podemos fazer com que a situação

possa ter algum tipo de participação ativa ou influência ou o papel ativo nesta questão? O que poderíamos fazer para realmente pressionar para termos mais participação ativa? Obrigado.

SUSAN CHALMERS: Obrigada, Kavouss. Quanto as pesquisas, temos sim o projeto DAAR, que aceita participantes voluntários no projeto. E essa é uma das maneiras, em que você se apresenta voluntariamente parar participar. Pode oferecer um arquivo de zona e também receber relatórios personalizados, mensais e treinamento e capacitação. Que são os recursos, que nós temos que podem ser de ajuda.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Obrigado, Samaneh. Outra pergunta ou comentário? Sim é um assunto fascinante. Poderíamos ficar o dia inteiro falando sobre isso. Mas eu passo a palavra agora ao Nick.

NICK WENBAN-SMITH: Obrigado. excelente. Sim, rapidamente, vamos ver o assunto sobre o qual vou falar, vou falar sobre o DASC, o Comitê Permanente de Abusos do DNS. Vou oferecer algumas ferramentas úteis, para ccTLDs.

E também como um projeto de base, inclui mais sobre práticas. E também pesquisas, achados no ccTLDs. E também agradecemos muito aqui, que vocês considerem participar hoje à tarde na sessão de 2 horas, em que vamos falar sobre ferramentas e medições de abusos. É uma questão complexa. E também vamos falar sobre os nossos futuros planos de trabalho nos próximos 6-12 meses.

Então agora que somos partes contratados, emendas, SubPro, gTLDs etc. Não, aqui, isso é uma coisa diferente. São códigos de país com muita diversidade, pelo que vemos aqui. E a minha função é que como representante do Reino Unido, faz 16 anos que eu trabalho nessas questões de ciberdelito, ciberabusos. E sou presidente desse Comitê Permanente para os Códigos de País.

E há uma enorme diversidade com IDNs. Mais 300 ccTLDs ao todo, inclusive incluindo as variantes de IDNs. É um grupo de pessoas muito interessante então. E não vamos ser contatados pela ICANN. Somos autônomos. E nós somos um órgão soberano com uma relação muito estreita com a ICANN, em que nós refletimos diferente culturas e países.

Então temos aqui... nós compartilhamos informações, não lidamos com políticas. Também tentamos entender e conscientizar. Também somos uma comunidade muito aberta. Promovemos o diálogo construtivo e aberto. E tentamos fazer o máximo possível para mitigar os Abusos do DNS, não apenas em um lugar, mas no mundo inteiro.

Quanto aos recursos, que fornecemos, temos aqui, o David McAuley da VeriSign, que tem recursos dedicados da VeriSign para a comunidade de ccTLDs. E realmente aqui, encorajamos os membros de compartilhar informações sobre esses recursos.

Também temos uma lista de e-mail para denúncias de abusos. Que vai ser outro recurso, para que a comunidade de ccTLDs esteja mais conectada, mais interligada. E uma... não é confidencial, mas é uma lista fechada de ccTLDs ou está restrita aos ccTLDs. Desculpem.

E aqui, uma pesquisa do DASC. Isso foi entre setembro e novembro de 2022. E tivemos 57 respostas únicas, algumas das quais refletem mais de um ccTLDs. Não é obrigatório responder essa pesquisa. É uma amostra de pessoas autosselecionadas.

E também para aumentar a participação. Tentamos filtrar quem vai participar. Para evitar ameaças, temos uma pesquisa que... e temos os detalhes aqui com três objetivos diferentes. Aqui, mostramos o que vamos fazer proximamente, para entender corretamente as atitudes e comportamentos na comunidade de ccTLDs.

E como eu disse antes, os ccTLDs são tão diversos mundialmente, são porque os países diversos, a diversidade de países. Sim, há diferentes ccTLDs de modelos de governança de registros em níveis de abusos. Há muita diversidade então.

E aqui, resumindo, na ICANN76, os resultados da sondagem mostram ações gerais, que tomam os ccTLDs, quando enfrentam Abusos do DNS. As práticas de mitigação, respostas. Os abusos sempre são diferentes. E é interessante, porque considerando o exemplo, não definimos o abuso, o que é Abuso do DNS. Temos os termos criminalidade. Temos o termo Abuso. E dependendo do que aconteceu, devemos então determinar se é criminalidade ou abuso.

É interessante isso. Muitos consideram os abusos com base nos riscos e outros automaticamente, suspendem o domínio ou desativa sem notificação prévia. Quanto a ICANN77 em Washington, tivemos diferentes modelos de registros. Porque alguns ccTLDs não permitem,

que seja criado um novo registro sem que antes sejam coletados outros dados de pré-registro.

E também tem essa correlação entre os dados do pré-registro e sua validação e os dados pós-registro. Ver se há alguma relação entre eles e Abusos do DNS. Foi fascinante, fazer esse exercício.

Então aqui, eu quero destacar é que há uma coisa dessa, que eu disse antes é que os ccTLDs são muito seguros. E quando há algum tipo de abuso, então é porque foi observado através de uma análise ou de uma autodenúncia. E também fizemos uma checagem das denúncias recebidas vis-à-vis os dados do nosso Instituto.

E temos uma sessão dedicada hoje à tarde, especificamente sobre como medir os abusos, como ferramentas e procedimentos disponíveis. E por que isso? É porque 38% dos que responderam, falaram que não estavam seguros e nem sabiam a quantidade de abuso, que um TLD tem para eles. Então por isso vamos fazer essa apresentação hoje à tarde. Todos então devem saber como quantificar os abusos, que eles sofrem. Então é isso que nós queremos ensinar, informar; que o pessoal esteja empoderado.

E um dos motivos dos quais o pessoal não sabia a quantidade de abuso, que tinha. É que em alguns pequenos ccTLDs... TLDs fazem muita checagem e registros, checagem de registros. Mas algumas são tão pequenas, que é muito difícil de detectar abusos. Os níveis de abusos são muito baixos. Às vezes, não há nenhum abuso, alguns meses. Outros, apenas um ou dois, o que é muito interessante.

Eu sempre fiquei meio suspeito sobre o modelo do registro gratuito. Porque isso foi interrompido, quando começamos a trabalhar. Uma hipótese é que os nomes de domínio muito baratos estão correlacionados a altos níveis de abuso. Então as os ccTLDs maiores, temos aqui em Hamburgo e um dos ccTLDs mais conhecido é .DE, muito eficiente.

Temos a Alemanha. É muito barato registrar. E os níveis de abusos são muito baixos. Então não é, não foi fácil comprovar a hipótese de que TLDs baratos estão relacionados a abusos. Então precisamos de aperfeiçoar então, os sistemas para ver como medir isso.

Então para encerrar, fizemos um webinar sobre... perguntamos sobre a variação entre os países. Para a maior parte dos ccTLDs, a definição de abuso não é limitada entre lacuna, entre abuso de conteúdo e abuso técnico. E como eu disse, níveis relativamente baixos para ccTLDs.

Há muita diferença da resposta do tratamento do abuso, mas tendemos de alguma forma a mitigar esse abuso. As validações ou verificações de registros são muito diferentes também entre regiões. Mas há muita validação. E nós, como custódios da base de dados nacional, nós todos queremos que esses domínios sejam bem protegidos.

E finalmente, bom... eu queria então dar uma prévia de hoje à tarde sobre a sessão sobre Ferramentas e Medidas de Abusos do DNS. Nós teremos excelentes apresentações do Instituto de Abuso do DNS. Há uma colaboração entre ccTLDs com as Equipes Técnicas da Holanda e da Bélgica, que estão colaborando para tornar as técnicas mais

eficientes, técnicas de inteligência artificial. Quanto a pergunta da China, no final teremos uma discussão entre mim e o Bruce Tonkin, que é vice-presidente do DASC e a Equipe de Liderança dos Registros de gTLDs. E vamos conversar então sobre o que, os pontos em comuns sobre Abuso de gTLDs e ccTLDs. Então não vale a pena, nós ccTLDs, sermos tão **[inaudível – 01:24:30]**, se nós estamos então fazendo com que o abuso vá para o lado dos gTLDs.

Então esses são os nossos planos para o futuro, que são políticas de registros, validação de dados, cooperação vertical entre registros e registradores; que pode ser usado como exemplo. E isso seria o final. Nós já temos com pouco tempo, eu passo para o Nico.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Muito obrigado. Alguma pergunta ou comentário sobre esse tema? Alguém perguntar algo ao Nick? Estou vendo que o Japão pediu a palavra.

NISHIGATA NOBUHISA: Muito obrigado. Eu tenho duas perguntas. A primeira. Eu vejo que há excelentes práticas para prevenir o Abuso de DNS nos ccTLDs. Há alguma forma de alavancar as boas práticas dos ccTLDs, para inspirar os gTLDs? Então quero dizer para antecipar-se ao Abuso do DNS.

A segunda pergunta é que eu vejo que há diversidade entre os ccTLDs, boas práticas. Você falou na Alemanha, por exemplo. Mas alguns países têm ccTLDs vulneráveis a condutas maliciosas. Vocês vão fazer mais

alguma atividade para estimular esses países, para que realize as atividades de prevenção?

NICK WENBAN-SMITH: Quanto a primeira pergunta, a nossa filosofia é... mostrar e não dizer o que as pessoas devem fazer. Nós todos... eu acho que a reputação é muito importante. Então incentivando melhores práticas, as pessoas veem os benefícios de ter uma boa reputação para a economia de tal, para o crescimento do país. E as pessoas copiam bons exemplos. E podemos compartilhar. Compartilhar bons exemplos em si melhora os padrões.

Em termos de gTLDs, nós não podemos criar políticas para gTLDs. Muitos dos bons gTLDs fazem mais do que o exigido no contrato da ICANN. Adotam as medidas voluntariamente, porque é bom e não porque é uma obrigação legal. E todos queremos então incentivar inovações e boas práticas.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Muito obrigado. Bons exemplos sempre são bons, a gente pode voltar ao tempo do Júlio Cesar. China, Taipei.

KEN-YING TSENG: Há alguma preventiva de Abusos do DNS diferente das adotadas pelos gTLDs?

NICK WENBAN-SIMITH: Bem, eu acho que há muitas coisas em comum, mas não se pode generalizar assim. Alguns gTLDs, .PHARMACY ou .BANK, quase não têm abuso, porque eles investem muito no registro. Alguns ccTLDs têm uma filosofia muito semelhante aos gTLDs. Então há muita sobreposição. Mas eu acho que não podemos dizer que coisas que só os ccTLDs fazem, que são melhores.

Eu fiquei surpreso que nos ccTLDs, temos apenas 10 vezes menos abuso do que em gTLDs. E eu quero saber o porquê isso acontece. Porque não consigo entender exatamente o porquê. Eu sei que os ingleses são muito honestos, por isso não temos criminosos. Então eu acho que alguma coisa está acontecendo. Então eu acho que temos que entrar em maior profundidade para saber o que é isso.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Então obrigado pela resposta. Chris Lewis-Evans.

CHRIS LEWIS-EVANS: Uma das coisas diferentes, que os ccTLDs fazem dos gTLDs é... nós temos um Centro de Informações. E isso é essencial para saber quais são os abusos, que estão ocorrendo, quais são as melhores práticas que podemos compartilhar entre os ccTLDs. Eu sei que o GAC já falou disso. Eu acho que esse ponto é muito importante.

NICK WENBAN-SMITH: É importante considerar cibersegurança. Seja em termos de resiliência da infraestrutura ou outros tipos de cibercrime. Nós temos que pensar nesta questão de forma mais holística.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Muito obrigado, Nick. Mais alguma pergunta? Bem, não há nenhuma pergunta online. Então, portanto, eu passo a palavra a Susan Chalmers, lembrando que você é a única pessoa, que está nos impedindo de almoçar é você. Estou brincando.

SUSAN CHALMERS: Agradeço a todos os oradores pelo seu tempo para nos trazer informações. Agradeço muito. Seja vocês, um usuário, solicitante ou registrante ou governo. Estimulem os... incentivem os registros e registradores a votarem a favor dessas emendas.

GULTEN TEPE: Desculpem, temos o Irã na...

KAVOUSS ARASTEH: Desculpem pelo almoço. Essa discussão foi muito útil e importante. Foi falado muitas vezes sobre cibercrime, ciberameaças, o impacto sobre o DNS. Eu estou um pouco surpreso, que outas áreas fora da ICANN, resistência de alguns governos nessa mesma reunião, de fazer qualquer coisa contra... ou para proteger a cibersegurança.

Então devemos ter uma única posição. Na ITU, houve um grupo sobre cibersegurança, lidando DNS. E houve rejeição de medidas. Então eu acho que deveremos ter a mesma posição e não ter duas posições diferentes em relação ao mesmo tema.

NICOLAS CABALLERO, PRESIDENTE DO GAC: Muito obrigado. Irã. Alguém gostaria de responder? Desculpem, não temos mais tempo. Obrigado pelos comentários, Irã. Peço um grande aplauso aos apresentadores de hoje. Bem, teremos agora o intervalo de almoço.

[Pessoa falando em inglês – 01:35:00]

[FIM DA TRNASCRIÇÃO]