ICANN81 | Assembleia Geral Anual – Discussão do GAC sobre atenuação do abuso de DNS
Terça-feira, 12 de novembro de 2024 – 10h30 às 12h TRT

DAN GLUCK: Senhoras e senhores, vamos começar. Olá, bem-vindos à Reunião do GAC sobre Mitigação do Abuso de DNS. Essa sessão está sendo gravada e é regida pelas Normas de Comportamento da ICANN e Antiassédio. Os comentários só serão lidos, se colocados no chat de Q&A. Teremos interpretação em todos os idiomas da ONU, mais português.

Levante a mão para falar e diga o seu nome e o idioma, em que for falar, se não for em inglês. Os microfones das mesas são apenas para os membros do GAC.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Bom, bem-vindos a todos à Sessão de Mitigação de Abuso de DNS. Nós temos a Martina Barbera, da Comissão Europeia; Owen Fletcher, dos Estados Unidos e a Hajime Onga, do Japão. Temos a honra de receber Mahmut Esat Yildirim, da Autoridade da Turquia, do ICT; Letícia Castilhos, do *Compliance* da ICANN, Reg Levy dos Registradores; Dennis Tan, dos Registros.

E, com isso, eu vou passar para o Hajime Onga, do Japão, que vai falar da nossa discussão.

HAJIME ONGA: Muito obrigada. Bom dia. Bem-vindos a esta sessão. Eu sou a Hajime Onga, o novo representante no GAC do Japão. E, nesta sessão, temos os nossos convidados da Turquia, do SSAC.

Esta é a nossa agenda de hoje. Teremos uma apresentação do país anfitrião. E, depois, a equipe da ICANN vai informar, vai dar uma atualização sobre o abuso do DNS e a implementação da emenda do Contrato de Registros e Credenciamentos dos Registradores. Então, teremos um tempo para discussão. E, depois, uma atualização do que foi discutido em Seattle.

Em primeiro lugar, a mitigação do abuso do DNS é uma prioridade para o GAC no Japão. Isso chamou muita atenção, especialmente em relação a *phishing*. Em segundo lugar, sobre o RA e RAA atualizado. Então, os registros e registradores dos gTLDs precisam relatar ou tratar as denúncias de abuso do DNS. Eles têm obrigações contratuais em relação a isso e, nesse caso, o abuso é definido como *malware, botnet, phishing, pharming* e, em alguns casos de *spam*. E, depois, vamos discutir as atividades no sistema do DNS como um todo.

Aqui temos o escopo da ICANN, quanto à mitigação de abuso. Então, o escopo da autoridade do RA e RAA é limitado. Os registradores da ICANN têm essa relação. Então, as ccTLDs não estão nessa caixa. E vamos discutir o que está nesse quadro verde.

Em primeiro lugar, em muitos casos de abuso de DNS e ccTLD, essa questão é prevalente na indústria do DNS e aqui em azul. E os criminosos usam provedores de hospedagem e CDNs. Aqui em vermelho, para mitigar o abuso do DNS, temos que cooperar.

No mês anterior, tivemos um webinar. E haverá uma introdução do SAC 115, que é uma das referências mais importantes do RA e RAA atualizados. O Jeff falou sobre o marco de mitigação do abuso do DNS e destacou a importância da cooperação entre a comunidade como um todo. Aqui, hoje, vamos discutir o que está no quadro em vermelho.

Comunicação, tecnologia. As tecnologias da comunicação e as autoridades vão falar sobre o tratamento do abuso do DNS e é importante aprender dos estudos de caso para determinar futuras medidas. E a representação vai apresentar as iniciativas da Turquia, incluindo a colaboração com condensadores de ccTLDs.

Depois, vamos discutir o que pode ser feito na ICANN. A ICANN vai falar sobre compliance de RA e RAA. Depois, teremos uma discussão, entre as partes, sobre os efeitos dessas emendas e teremos uma discussão do GAC, considerando essa discussão anterior. E depois, a ver o que pode ser feito no ecossistema.

A agenda, então, é bem cheia. Então, eu gostaria de passar, então, para o senhor Mahmut Yildirim, da Turquia.

MAHMUT ESAT YILDIRIM: Muito obrigado. Olá a todos. Eu sou Mahmut Esat Yildirim. Eu sou do Departamento de Informações e Tecnologias da Autoridade da Turquia. Vou falar sobre mitigação de abuso do governo da Turquia, em relação a CERT e ccTLD.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Poderia falar mais perto do microfone?

MAHMUT ESAT YILDIRIM: Bem, o CERT Nacional da Turquia e o ccTLD, que é o .TR, estão no mesmo departamento. E o TR CERT é a Equipe de Resposta a Emergências da Turquia e lida com as respostas a incidentes de cibersegurança. O ccTLD TRABIS está no mesmo órgão. Então, é por isso que podemos combinar duas atribuições ao mesmo tempo para combater ameaças ao DNS.

Nós temos quatro estratégias e planos de ação. Alguns destaques nesses documentos para detectar e mitigar mecanismos de abuso, quanto a ciberataques ou ciberameaças. Essa é a última versão que tem quatro temas, seis objetivos estratégicos, 18 alvos e 61 itens de ação.

Esses pontos, então são a abordagem de cibersegurança centrada em humanos, o uso seguro de tecnologias para cibersegurança, resiliência, tecnologias nacionais para combater as ciberameaças, ter um sistema de defesa proativo e a base jurídica para mitigar o abuso do DNS e ciberameaças.

São implementadas de acordo com as cláusulas dos artigos da Lei de Comunicações Eletrônicas da Turquia, no artigo 60, parágrafo 11, diz que a organização ou alguém deve tomar todas as medidas necessárias para proteger e impedir ciberataques a organizações governamentais, privadas e entidades reais. Essas são as responsabilidades do CERT da Turquia.

O artigo seguinte diz que a organização pode receber e avaliar informações, documentos, dados, dentro do escopo da sua

responsabilidade. E com essa lei podemos solicitar dados para detectar os ciberataques a diferentes organizações ou de diferentes sistemas.

A base legal do ccTLD, e dentro do marco das regulamentações, e o ccTLD, então apoia as forças da lei no combate ao ciberdelito e fornecemos informações solicitadas pelas autoridades. Como os tribunais, por exemplo, às vezes trabalhamos intimamente com as forças da lei e os tribunais para impedir atividades de abuso.

E quais são os abusos que nós tratamos quase todos os dias? *Phishing, malware, spam*, sequestro de domínios, *botnets, Command and Controls*, materiais de exploração infantil, fraudes, abuso do DNS, como sequestro ou spoofing do DNS e também violação de privacidade. Estamos tentando detectar e impedir essas categorias. E desenvolvemos ferramentas e mecanismos para detectá-los.

A primeira dessas ferramentas é o AZAD, é um projeto, é um software interno que usa um mecanismo de IA, para detectar phishing. Estamos coletando todos os *feeds* de domínios, recentemente gerados e de outras fontes. São milhões de nomes de domínios todos os dias. E através da inteligência artificial estamos reunindo, na verdade, coletando os nomes de domínios de phishing, ou detectando em meio a milhões de nomes de domínios para que os operadores do ccTLD possam verificar manualmente, se o phishing é ou é de fato.

E o sucesso desse software é de 97%. Então, geralmente, esse phishing é detectado e bloqueado antes de se tornarem ativos. Então, trabalhamos juntos com os ccTLDs e com os ISPs também para que, de fato, possamos mitigar o phishing. Todos esses conteúdos

relacionados a abusos são coletados por software específico interno e que são, então, notificamos as diferentes divisões.

Então, qual é o fluxo do abuso? Então, coletamos notificações de diferentes fontes: registrantes, registradores, usuários finais, AZAD também. Tudo isso é colocado no aplicativo KULE, que passa para o TRABIS dos ccTLDs. E analisamos os documentos utilizando o IA, para que os ccTLDs possam superar o problema.

Estatísticas do nosso KULE, o software, 13.000 denúncias foram coletadas. Dessas, 8.000 são um incidente para nós. Isso significa que devem ser verificadas, se é caso de abuso ou não. Desses 8.000, 5.000 de fato eram abuso e o domínio foi bloqueado ou suspenso. Até agora, encontramos mais de 900 sites de phishing, mais de 3.400 sites de phishing de *banking*, 3 de malware, de comando e controle e de emissão de nomes.

Há padrões comuns, como denúncias. Talvez em inglês, isso não faça sentido. Mas a implicação da denúncia utiliza uma solicitação de cancelamento e um número ou é necessário fazer um empréstimo e esse número é usado pelos bancos. Então para registrar é necessário fazer um pagamento. Essas informações de pagamento são ligadas aos nomes dos bancos e, portanto, os criminosos não podem utilizá-los.

Temos aqui essa oportunidade de ter uma campanha online contra atividades de phishing ou abusos. Talvez em inglês isso não faça muito sentido. Mas nós estamos melhorando nossos mecanismos e aumentando a quantidade desses tipos de palavras a cada dia,

ensinando novos mecanismos e novas palavras para melhorar o mecanismo de AI para detectar abusos.

Então, o TRABIS foi estabelecido em 2022 e houve depois alguns pontos de inflexão depois desse ano. E antes do TRABIS, todos os registros baseados em nomes eram baseados em documentos com .TR ou NET.TR. E era necessário fornecer um documento oficial, mas depois do TRABIS, isso melhorou e também melhoramos assim os nossos mecanismos de detecção. Depois de 2023, começamos utilizando as capacidades do CERT juntamente com o TRABIS, para mitigar isso mais rapidamente.

Os métodos de denúncia podem ser feitos por e-mail, através do site, do *Search* ou de uma linha telefônica gratuita para denunciar essas atividades. Então, temos uma lista negra, que é pública e disponível para todos e que compartilhamos com o mundo para poder implementar essas listas negras de interesses IP, nomes de domínio, *malware, phishing*.

Então, estamos abertos para colaborar com os membros do GAC e tentar encontrar políticas mais efetivas de mitigação de abusos. E gostaríamos de saber como os outros países lidam com isso, com os outros ccTLDs. E podemos compartilhar as nossas experiências, também gostaríamos de contribuir com as nossas experiências sobre como implementamos essas políticas ou mecanismos. Então, é isso. Se houver alguma pergunta, estou aqui à disposição. Muito obrigado.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Obrigado, Mahmut. Então, deixamos agora o espaço para perguntas e respostas. Temos algumas perguntas, eu tenho algumas perguntas sobre os tipos de técnicas que vocês estão utilizando agora para identificar anomalias no tráfego do DNS ou nas consultas ou no *spam* em geral.

Que tipo de IA, que técnicas de IA são as que melhor funcionam para vocês de acordo com a sua experiência? O Random Forest, talvez? Ou *Deep Learning*? E, nesses casos, que tipos de *Deep Learning*, vocês utilizam? Redes convolutas, por exemplo? Para ter uma ideia aqui do que realmente dá certo para vocês aqui na Turquia.

MAHMUT ESAT YILDIRIM: Obrigado. Eu gosto muito desse aspecto tecnológico. E temos dois aspectos aqui diferentes nessa missão de processo de aprendizado. Temos métodos de aprendizado para detectar os nomes de domínio recentemente registrados e verificar similaridades. E, por exemplo, eu registrei MAHMUT.COM e nossos modelos verificaram que há 90% de phishing envolvidos com esse nome. Estamos trabalhando com o Random Forest.

E também trabalhando com os ISPs, que têm um certo poder, com o CERT. Estão utilizando também os seus próprios sistemas de redes. Também sistemas, um importante sistema de redes de ISPs para detectar outros tipos de abusos do DNS. E também sequestros, ataques às redes. E também, quando é detectado um ataque, ele é denunciado. E temos especialistas em ccTLDs, que dão uma resposta a essas denúncias de ataques.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Muito obrigada. Comissão Europeia. E depois é Mustafizur.

GEMMA CAROLILLO: Obrigada ao colega da Turquia pela tão interessante apresentação. Eu tenho algumas perguntas, porque também na União Europeia, temos o nosso próprio CCTLD.EU com uma abordagem similar, utilizando IA e aprendizado por máquinas para evitar o registro de nomes de domínio maliciosos.

Mas a sua abordagem parece ir além, bem além disso. E, pelo que entendi, vocês integram tecnologias de inteligência com o CERT e podem trabalhar de forma preventiva, detectar, então, antecipadamente.

Eu não sei se essas são informações que você pode compartilhar aqui. Nós discutimos muito sobre isso no nosso grupo. Isso está sendo desenvolvido internamente pelos ccTLDs. E se você tem alguma informação de custos desse sistema, seria muito bom para considerar integrá-los facilmente com outros registros.

MAHMUT ESAT YILDIRIM: Sim, obrigado. Se nossos mecanismos CERT, em geral, utilizamos os próprios desenvolvedores internos e levou aproximadamente um ano, desenvolver esse mecanismo. Talvez poderia ser menos, mas no nosso caso, foi mais de um ano para ensinar os algoritmos, as máquinas e criar novos modelos. E também, antes desse algoritmo, fazíamos isso, os operadores faziam isso manualmente através de rótulos, os *tags* de

nomes de domínio, como *Phishing Malware*, e fazendo uma lista de domínios rotulados. Isso era melhorado a cada dia, foi bem sucedido.

Mas, por outra parte, com o mecanismo CERT, como você mencionou, ele prevê diretamente as atividades de abuso. O ccTLD pode detectar abuso, ou alguém pode notificar um ccTLD. Temos um site de *phishing*, ou eles podem detectar. E com o CERT, através de cooperação com os ISPs, em cinco minutos podemos bloquear o acesso a esse nome de domínio, ou cancelar também, ou eliminar, desativar, e isso depende de cada caso. É uma funcionalidade que atua por comando e controle para bloquear diretamente em nível de ISPs.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Muito interessante. Temos Bangladesh e a Índia. Por favor, sejamos breves e precisos.

MUSTAFIZUR RAHMAN: Obrigado pela maravilhosa apresentação e como você mencionou, depois de ter verificado a documentação, a quantidade de denúncias foi reduzida. Então, como é que vocês fazem, obtém um equilíbrio para fazer com que o serviço seja rápido?

MAHMUT ESAT YILDIRIM: Se isso foi antes do TRABIS, em 2022, e eu já falei antes que esse é um processo muito lento, você tentava registrar-se com .COM.TR seu domínio. Tinha um documento de 4 ou 5 páginas, os operadores

deviam verificar esses documentos através de diferentes mecanismos. E depois, em 2022, não é tão lento assim. Agora é rapidamente, vai por ordem de chegada, e não exigimos documentos.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Obrigado. Então, temos a Índia.

T. SANTHOSH: Obrigado, Mahmut, pela apresentação. O .TR está aberto para o mundo? Se for afirmativo, qual é a validação de verificação, que vocês utilizam?

MAHMUT ESAT YILDIRIM: Sim, o .TR está aberto para o mundo, mas temos uma série de registradores, autorizados na Turquia. E vocês só podem recorrer a eles e não, a outros. E vocês devem ter... os dados do WHOIS devem ser corretos, oferecer dados corretamente, o e-mail, endereço postal, telefone, os dados devem ser acurados. É a mesma coisa, que com os outros gTLDs.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Uma última pergunta, me desculpem, mas antes de passar para o Fletcher. E quanto a tunelação do DNS, que funcionou melhor de acordo com a sua experiência? O que é que funcionou melhor? Como uma percepção multicamada em termos de redes neurais, ou então, o que funcionou melhor?

MAHMUT ESAT YILDIRIM: Eu acho que ao utilizar esses dados de fluxo e as redes neurais, isso pode funcionar melhor. Porque não sabemos, com certeza, como é implementado essa tunelação, os mecanismos de túneis do DNS. E podemos, sim, coletar os pacotes, sim, reuni-los, e obter outros pacotes, utilizar redes neurais para ensinar, para detectar túneis no DNS. E como são muitos pacotes, um conjunto muito grande de pacotes, que nos permite analisar em detalhe.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Fala, Bangladesh? Não, era de antes. Tinha pedido a palavra. A Líbia. É a vez da Líbia.

KHALED ALTARHUNI: Obrigado. A pergunta é para a Mahmut. Obrigada, Mahmut, pela sua excelente apresentação. Gostaria de saber, esse sistema pode resolver o conteúdo ilegal?

MAHMUT ESAT YILDIRIM: Sim. Esse software que nós criamos, o AZAD, eu não o mencionei em detalhe, mas verifica de forma similar com os nomes do domínio, e também os contextos desse site. Primeiro tem um alarme, um sinal, e quando detecta que é isso, em uma verificação de similaridade, 95% é o *phishing*, que deflagra esse alarme. E não há contexto para esse site, portanto não podemos fazer nada sobre isso. Por exemplo, uma pessoa tem uma arma na mão, isso não significa que ela esteja por matar alguém.

E por isso devemos primeiro identificar se é abuso nesse site, e as verificações de algoritmos e aprendizado, ou o contexto do site, é isso, que deve ser renovado ou atualizado para detectar as atividades abusivas no contexto, como um site de *phishing* e outros tipos de coisas, que medem e evitam isso.

OWEN FLETCHER: Está acabando o tempo para essa sessão, vou ser breve e vou tentar ser rápido, mas temos aqui o representante de *Compliance* na ICANN, Leticia Castilho, e quem vai apresentar uma atualização sobre as Emendas Contratuais no GAC, e os impactos.

LETICIA CASTILLO: Fala Leticia Castilho, Diretora Sênior de i da ICANN. E como falou o Owen, eu vou aqui falar sobre o que aconteceu depois de seis meses da aplicação dessas emendas de contratos de abusos, contra abusos. Semana passada publicamos um relatório descritivo sobre esses seis meses de aplicação, 17 páginas, muita informação sobre as pesquisas feitas, os resultados, as conclusões, respostas. E, portanto, leiam o relatório se vocês desejarem ter mais informações sobre as ações tomadas de aplicação.

E vamos para os dados. De 5 de abril de 2024 até 5 de outubro de 2024, iniciamos 192 investigações com registradores e registros sobre abusos do DNS. E, nesses casos, tínhamos pelo menos um tipo de abuso do DNS, que é o *phishing, pharming, malware botnet*, ou *spam*, quando é utilizado como vetor de um dos outros quatro modos de abusos. Em duas dessas investigações, houve um aviso de infração formal por um

operador de registro e um de um registrador, por não ter cumprido os requisitos do DNS.

E resolvemos 154 investigações de abusos através da nossa resolução informal, o nosso processo. Estamos resolvendo todos os tipos de abusos. Isso porque o registrador e o registro demonstram estar em conformidade ou agir para remediar as infrações.

E porque um caso de *compliance* poderia envolver um nome de domínio, ou vários nomes de domínios, ou porque, às vezes, há mais domínios numa mesma conta, que estão sendo utilizados de forma maliciosa. Portanto, essas 154 investigações levaram à suspensão de mais de 2.700 nomes maliciosos e também foram desativados mais de 350 sites. Porque em alguns casos o registrador também fazia serviços de *hosting*.

Portanto, estes são os valores para os últimos seis meses, de 5 de abril a 5 de outubro de 2024. Temos várias pesquisas agora em andamento e concluídas, que não estão aqui, mas que serão, sim, incluídas na próxima atualização.

Durante esses seis meses, também participamos de muitas atividades de divulgação e comunicação para conscientizar a comunidade sobre esses novos requisitos. Em setembro, por exemplo, participamos de uma oficina com partes contratadas em Beijing, em que falamos sobre diferentes requisitos e recomendações sobre abusos. Também aqui em Istambul, no mês passado, trabalhamos com os colegas do GDS e GSC em atividades de capacitação, como parte do foco múltiplo e variado do Programa de Mitigação de Abusos do DNS.

Lançamos também uma auditoria para validar o cumprimento do RAA e não só sobre requisitos e abusos do DNS. E em junho, começamos a publicar relatórios mensais sobre o cumprimento efetivo desses requisitos.

E ações de aplicação começaram em abril de 2024 e são atualizadas mensalmente. O formato desses relatórios dá uma visão ampla desses casos, que são complementadas com atualizações. A intenção sempre é continuar melhorando esses relatórios e entregá-los à comunidade e receber ` da comunidade. Eu mencionei o relatório de 8 de novembro.

Eu mencionei anteriormente os 154 casos resolvidos. Esse slide mostra as razões da resolução, 151 foram ligados a registradores e 52% dos casos foram confirmados abusos e a resposta foi considerada inconformidade. Porque nos deram uma explicação razoável do que foi feito para investigar e qual foi a sua conclusão.

Por exemplo, no registrador avaliado, todas as informações e provas, que tinham em relação ao nome de domínio, determinaram que o registrante estava atuando com o conhecimento e consentimento da entidade, que foi falsificada.

Por exemplo, 12% dos casos, o registrador tomou medidas para interromper o abuso do DNS. E em aproximadamente 3% dos casos, o registrador tomou outra medida, redirecionando o serviço de nomes ou usando *sinkholing*. Então, isso em relação aos registradores.

Agora, quanto aos registros, nós resolvemos 3 casos de abuso do DNS com operadores de registro. Todos os casos foram suspensos pelo registro, dos nomes de domínio. Alguns estão em andamento. Tivemos

também um com problemas do contato, do abuso, mas foram todos solucionados. A diferença de números entre registradores e registros se deve ao fato, que de todas as denúncias recebidas, 94% se referiram aos registradores.

Nós não temos o mínimo ou o máximo para iniciar ou dar andamento a uma investigação. E durante esse mesmo período, enviamos uma notificação formal de violação a um registro e uma a um registrador. Nós temos ainda muita coisa que está em andamento e muito já foi resolvido depois do dia 5 de outubro e isso será atualizado no próximo relatório. Então, se tiverem alguma pergunta.

OWEN FLETCHER: Muito obrigado. Eu acho que foi muito útil ter recebido essas informações e isso é importante para o GAC. Eu não sei se há perguntas do público.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Sim, temos tempo para algumas perguntas. Índia.

T. SANTOSH: Essa apresentação explicou brevemente o papel dos registros e registradores. Durante esse período na Índia, fizemos três denúncias, mas ainda não sabemos qual é a situação disso. Então, qual é a situação da denúncia, que nós fizemos e nós não temos resposta nem por e-mail?

LETICIA CASTILLO: Se eu entendi, você fez três denúncias e você não recebeu nenhuma atualização sobre a situação? É isso? Eu acho, que eu sei do que você está falando e eu acho que nós pedimos mais tempo para dar uma resposta. Mas eu posso olhar isso com você depois, mas é parte de um processo.

Uma denúncia é feita, há uma confirmação, que dá um número de identificação do caso. E há comunicações tradicionais, de que o processo está em andamento ou solicitação de mais informações. Isso acontece frequentemente.

Muitas vezes precisamos de mais evidências de um denunciante. Muitas vezes a gente recebe denúncias do mesmo denunciante, várias vezes. Então, em geral, quando o caso é resolvido, o denunciante recebe uma informação, de que o caso foi resolvido e também há informações de como entrar em contato com o *Compliance*. E eu posso conversar depois com você sobre isso.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Países Baixos, agora.

ALISA HEAVER: Muito obrigada pela apresentação. Eu queria saber, há uma comparação desses números hoje com os de um ano atrás, quando essa emenda ainda não havia sido implementada? E queria saber qual é a duração média de uma investigação, antes que o registrador tome alguma medida?

LETICIA CASTILLO: Então, foram feitas mais investigações a partir da implementação da emenda. Quanto aos números dos últimos anos, até 5 de abril, vemos que houve um aumento das denúncias de abuso. Em 2023, recebemos uma média de 1.300 denúncias a mais. De janeiro a 2024, a média foi de quase 2.000 mensalmente.

Quanto à duração da investigação, depende do tipo de investigação. Casos de abuso de DNS, em que há um nome de domínio, contatamos o registrador. Já nos informam. É muito simples, já suspendemos o domínio.

Mas há investigações, em que há milhares de nomes de domínios envolvidos. Então, às vezes detectamos que há um padrão, que indica que eles não têm um tratamento padronizado para o tratamento de abuso. Então, solicitamos um plano de mitigação e queremos, então, que haja indicadores. Então, nós pressionamos esse registrador, para que tomem medidas. Isso depende de cada caso.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Uma pergunta.

LAUREEN KAPIN: Como membro do Grupo de Segurança Pública, eu quero agradecer todo o trabalho, que está sendo feito e é muito animador ver que essas respostas muito específicas à mitigação do abuso do ADNS estão sendo feitas.

A minha pergunta é, quando um registrador tomou uma medida para interromper o abuso do DNS, que não é a suspensão do nome de domínio?

LETICIA CASTILLO: Bem, as ações dependem das circunstâncias específicas indicadas. Há casos claros, então, em que o nome foi registrado para perpetrar abusos. E eu penso num caso em especial, que houve um nome comprometido. O registrador foi contatado e foi avisado do que está acontecendo. Você tem que fazer tal coisa para garantir, que isso não continue a acontecer. E isso foi feito pelo próprio registrador.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Eu passo, então, de volta ao Owen.

OWEN FLETCHER: É muito bom saber, que essas métricas estejam sendo publicadas sobre a implementação da emenda dos contratos. Então, agora passamos por uma discussão. No painel nós temos o Reg Levy da Tucows; o Dennis Tan da VeriSign e o Jeff Bedser, do CleanDNS. E vão responder algumas perguntas, que estão nesse slide.

O Dennis disse, como parte contratada, o que você fez desde a emenda? Quais foram os impactos e as consequências das emendas? E quais foram as lições aprendidas nesses três meses desde a implementação? Então, desculpem, eu vou interromper, se vocês passarem de três minutos, porque esse é o tempo alocado. Eu vou começar com o Reg.

REG LEVY: Reg Levy da Tucows. A Tucows se envolveu na negociação da emenda. Eu não tenho muito, eu quero dizer que nós não mudamos muito desde a emenda. Então quer dizer que estávamos trabalhando corretamente. E tenho satisfação de dizer, que agora somos parte, essas emendas já fazem parte das obrigações contratuais. Nós temos uma equipe de sete profissionais para o abuso do DNS e tomar medidas de mitigação.

O que nós vimos é que nós começamos a fazer sinkholing, em vez de suspender. *Sinkholing* significa que dirigimos os registros de DNS para um domínio com um conjunto especial de servidores DNS, que são rodados pelo CleanDNS, para que possam obter mais informações. Para ver quais são as tendências entre os registradores. Grupos, como o CleanDNS, podem detectar tendências mais amplas no setor. E nós, com isso, queremos obter mais informações para identificar essas campanhas de abuso.

OWEN FLETCHER: Denis.

DENNINS TAN: Muito obrigado, Owen. Não tenho muito mais a agregar, do que o Reg disse em termos de operadores de registro. Grande parte da sua responsabilidade está... depende dos registrantes, que têm relação direta com... dos registradores que têm contato direto com os registrantes. Por exemplo, no *botnet*, nós estamos utilizando engenharia em termos de nomes de registro.

E, geralmente, consultamos os registradores, para que trabalhem com os registrantes de forma adequada para mitigar o abuso. E, em geral, e falando em geral para operadores de registro, um dos aspectos das emendas é que nós melhoramos a qualidade das denúncias de abuso, o que torna mais fácil avaliar e determinar qual é o abuso e, assim, tomar as medidas adequadas.

O nosso grupo combina... tem um grupo de trabalho de CPH e DNS. E eu acho que essa emenda será um primeiro passo de várias atividades para ajudar a mitigar o abuso do DNS. Estamos fazendo divulgação com outros grupos da ICANN, para identificar problemas em comum e ver se há uma questão de políticas ou encontrar melhores práticas.

Essa semana, eu participei de uma reunião com o NCSG. E isso é um exemplo dessas atividades de relacionamento da nossa comunidade dentro da ICANN.

OWEN FLETCHER: Vamos para o Jeff, para os slides.

JEFF BEDSER: Muito obrigado. Bom, essa é uma repetição do que foi mencionado antes. Mas aqui, só um pouco de comparação de dados. Desculpem pela minha voz, espero que possam me entender. Eu tenho dados para compartilhar sobre grandes volumes de abuso do DNS, para termos uma perspectiva dos volumes sobre os quais estamos falando.

De abril a junho, processamos 628.000 denúncias de abusos, que representam quase 60.000 nomes domínios únicos. E o volume mensal

antes dessa mudança nas obrigações era de 225.000 por mês. E depois dessas novas obrigações, observamos um aumento e alcançamos quase 240.000 denúncias mensais.

Eu conversei com registros, registradores e empresas de *hosting*, e eles veem esse aumento, porque agora houve uma mudança nas obrigações, e são geradas mais denúncias, talvez, ou relatórios de denúncias. E às vezes temos três relatórios, triplicados com a mesma denúncia.

Vemos aqui um relatório de *phishing* de outubro de 2023 até setembro de 2024, os relatórios, as denúncias aumentaram muito, mas em geral o volume das denúncias se mantém no mesmo nível no que tange ao *phishing*.

Isso aqui é muito interessante, tivemos uma denúncia do registro de .TOP. Foi uma informação pública, foi notificado sobre o descumprimento com 70.000 denúncias de abuso de .TOP. Em agosto subiu, em setembro ainda mais, e em outubro alcançou 13.000, o que é um exemplo muito bom de *Compliance* da ICANN.

Porque, apesar do aviso de descumprimento, o volume das denúncias da DSTLD.TOP continuou aumentando. Portanto, o *Compliance* está realmente realizando o seu trabalho bem e com os abusos, e são esses volumes aqui, o que demonstram isso.

Estamos medindo a quantidade total de denúncias processadas, de domínios envolvidos, com uma proporção de 3 a 1 ou 2 a 1. E a relação entre denúncias e domínios, também a quantidade de ações, que implementam *Compliance* por cada registro, entre outras medidas.

O que deveríamos medir? Devemos mudar comportamentos para obter mais mitigação e ver quantas denúncias realmente demonstram efetivamente a mitigação e as ações implementadas. Porque, na metade dos casos, não é iniciada nenhuma ação.

Se os danos foram mitigados antes das denúncias, por exemplo, devemos ver se, com essa nova maneira de obter provas, ver o que aconteceu realmente, quanto é que o prejuízo durou, por exemplo. Isso porque, obviamente, se o nome do domínio tem um ciclo de vida mais breve, menor será o número de vítimas. Podemos utilizar inteligência artificial e aprendizado automático e reduzir o tempo da validação da denúncia até a ação de mitigação.

Depois, devemos considerar algo que são as métricas, o *Domain Metric*, e a ICANN está trabalhando com isso, com o Diretor de Tecnologias. E ver quão efetiva foi a mitigação, quanto à redução do volume total. Também ver o que acontece com a mitigação e com o comportamento dos delinquentes. Depois, quanto esforço foi dedicado para que uma parte contratada, que estava descumprindo pudesse modificar seu comportamento.

OWEN FLETCHER: Jeff, desculpe, mas está acabando o tempo.

JEFF BEDSER: É esse, é meu último slide aqui. E a mudança nas obrigações foi muito boa, mudanças de comportamento, isso também está dando resultados bons. E as partes problemáticas fora do ecossistema não

estão agindo, estão sendo avisadas muito mais para mencionar aqui. Mas as emendas estão tendo impacto no sistema e depois de seis meses de implementação, acho que as conclusões são positivas.

OWEN FLETCHER: Sim, também temos aqui uma declaração de Mukesh Chulani da ICANN, que trabalha em Domínios e Estratégias da ICANN.

MUKESH CHULANI: Observamos um impacto em nível de casos, o impacto dessas emendas, se passaram sete meses desde a sua implementação. Já ouvimos as partes contratadas, observamos relatórios consolidados da Equipe de *Compliance*, também relatórios de terceiros, especialistas em métricas, portanto, observamos que há impactos positivos.

E essas emendas não foram concebidas como uma solução definitiva, mas sim como um primeiro passo. E vamos continuar mudando no futuro e devemos seguir tudo isso, continuar dialogando.

E sob a nossa perspectiva, *Compliance*, deve exigir o cumprimento das obrigações contratuais. Temos dados e contratos focados nos casos existentes. E isso deveria ser complementado com uma perspectiva mais ampla do mercado e o que acontece com o abuso. A Equipe da OCTO da ICANN tem uma métrica, que é uma plataforma para coletar medições de dados.

E nos próximos dias e meses teremos mais informação. Temos também o Projeto INFERMAL, que avalia as preferências dos atacantes. Estamos trabalhando internamente, como a Leticia mencionou, estamos

observando tudo isso, ver como mudar e introduzir melhores práticas através de plataformas. Obrigada pelo convite.

OWEN FLETCHER: Obrigado, Mukesh. Acho que é muito útil receber essas informações, investigações e análises de um amplo leque de atores, de maneira que o GAC tenha essa informação, que possa depois ser introduzida nos próximos debates. Temos um tempo agora para perguntas e respostas antes de passarmos ao debate do GAC.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Obrigado, Owen e Mukesh, os painelistas também, Denis e Jeff, Reg. Eu não vejo aqui no Zoom ou aqui de forma presente, que solicite a palavra. Portanto, a Martina que vai liderar o próximo bloco.

MARTINA BARBERO: Alguém pediu a palavra?

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Comissão Europeia.

GEMMA CAROLILLO: Obrigado, Nico. Tenho uma pergunta para a pessoa da VeriSign. Você mencionou que estão analisando uma possível elaboração de políticas. Falou sobre o relacionamento com a comunidade. Portanto, gostaria de saber se você já tem alguma ideia de como é isso? Porque no GAC estamos analisando a mesma ideia.

DENNIS TAN: Muito obrigado pela sua pergunta. Não vamos necessariamente fazer um processo de elaboração de políticas, porque a comunidade mencionou, nos disse que o processo é lento, requer muitos recursos e muito tempo. E agora eles estão se concentrando em PDPs mais específicos e limitados. Sim, o PDP poderia ser uma solução possível. Estamos conversando com a comunidade da ICANN. E gostaríamos de ver mais os detalhes, ler em detalhes o relatório do Projeto INFERMAL, que será muito útil e que iniciará novas rodadas de conversas.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Dou a palavra para os Estados Unidos.

OWEN FLETCHER: Sim, eu acho que a Diretoria ofereceu organizar sessões de escuta sobre o escopo dos possíveis PDPs no futuro, para ter considerações com maior nível de nuance para o futuro. Isso é interessante, podemos acompanhá-lo.

REG LEVY: Em representação do grupo reduzido de abuso do DNS. Dennis e eu somos copresidentes desse subgrupo, ou Pequeno Grupo, que está dentro do setor de partes contratadas. Já tivemos algumas dessas sessões de escuta, que não são as da Diretoria. Mas dialogamos com diferentes grupos da comunidade para determinar o que eles querem que nós façamos, o que é interessante para eles, e que, como partes contratadas, possamos reiniciar essas iniciativas. Talvez não um PDP.

E já nos reunimos com o ALAC. Vamos nos reunir com o SSAC para dialogar individualmente com cada grupo da comunidade, para que cada grupo tenha a oportunidade de dialogar conosco.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Obrigado. Obrigado, Estados Unidos. É o Reg. E pediu a palavra a Martina Barbera da Comissão Europeia, quem vai falar sobre os próximos passos e as considerações para o *Communiqué* do GAC.

MARTINA BARBERO: Temos duas partes breves na agenda, que, antes do almoço, são partes importantes. E gostaríamos de falar primeiro sobre os assuntos que ouvimos hoje e preparamos algumas perguntas para vocês. Gostaríamos de perguntar, se vocês têm alguma opinião sobre o que falamos hoje, sobre a implementação e impactos das emendas nos contratos por abusos?

E esse seria um bom momento para compartilhar dúvidas também, se houve lições aprendidas da rodada anterior e como prepararmos em termos de prioridades para a próxima rodada. E ontem falamos dos PICs nas partes contratadas, eu não estive, mas sei que há um relatório muito bom sobre o abuso do DNS da rodada anterior com conclusões, que poderiam ser úteis para a próxima rodada.

E depois ouvimos uma apresentação excelente dos colegas da Turquia. E gostaria se há alguma melhor prática de ccTLD, que poderíamos considerar para pensar mais sobre o espaço do gTLDs. Antes de passarmos às considerações do *Communiqué*, gostaria de saber se

alguém aqui no GAC, quer fazer algum comentário com base a essas perguntas.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Obrigado, Martina. Sim, vamos responder perguntas, comentários, o que vocês quiserem compartilhar conosco agora. Índia.

T. SANTOSH: Na ICANN80 tivemos uma proposta para a implementação do DNS, que deveria ser obrigatório, especialmente nos setores de serviços financeiros, saúde, governo e telecomunicações. Isso significaria estar em linha com medidas de segurança mundiais e garantir a proteção de interesses nacionais vitais. Então gostaria de ouvir algum comentário sobre essa implementação.

REG LEVY: O DNSSEC é uma maneira de segurar os nomes de domínio, HTTPS, que parece que atualmente adotou o protocolo de segurança. E foi decidido pelo mercado, é muito bom e realmente oferecemos o DNSSEC, com muito prazer, para alocar o DNSSEC para qualquer nome de domínio, que for comprado por nós. Isso não é uma opção muito popular, mas temos clientes interessados e também o HTTPS parece estar sendo utilizado. E há *browsers* que também estão começando a exigir também o HTTPS.

Não há nenhum problema e alguns setores poderiam buscar vias, outras vias de segurança. Mas eu vi que a maioria dos clientes não estão interessados no DNSSEC dessa maneira.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Obrigado. Reino Unido pediu a palavra.

CHRIS: É a primeira vez que estou na ICANN, sou representante do Reino Unido. Sou o Chris, trabalho com o Grupo de Segurança Pública, especificamente. E quanto ao comentário da Índia, sob uma perspectiva mais geral. Na sexta-feira passada, sob a presidência do Conselho de Segurança da ONU, por esse mês, do qual fomos os presidentes. Houve uma sessão sobre *Ransomware* e sobre o impacto no setor da saúde. E realmente houve um interesse muito grande nessa questão entre os membros.

E esse interesse foi demonstrado por diferentes órgãos. Não é uma pergunta, aliás, é mais um comentário sobre outros órgãos, encontros multilaterais e governos, que estão realmente considerando cada vez mais essas questões na sua agenda. São bastante pertinentes e, portanto, acho que nesse Grupo de Trabalho de Segurança em que trabalhamos, realmente estamos colocando cada vez mais o foco nesses setores, especificamente dos CNI.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Muito obrigado, Reino Unido. Agora os Estados Unidos.

OWEN FLETCHER: Gostaria de responder brevemente sobre o DNSSEC. Eu me lembro que na ICANN80, incluímos um texto no *Communiqué* de acordo com a

solicitação do Santosh, naquele momento. E poderíamos rever esse texto, mas também gostaria de destacar que esse texto colocou o foco no apoio, em apoiar a adoção do DNSSEC, que é bom para identificar. Não me lembro muito bem sobre qual foi a ideia exata, mas foi algo que deveríamos considerar para termos mais informações e submetê-las à consideração.

Também me lembro de que o SSAC, o DNSSEC, observou na sua reunião bilateral conosco, que esse tópico é muito importante.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Obrigado, Reino Unido. Então passo para Martina Barbeiro, da Comissão Europeia, sobre os próximos passos e considerações que devemos levar.

MARTINA BARBERO: Agradeço a todos que participaram hoje. Então, com isso, nos leva às considerações do *Communiqué*. Lembrando elementos possíveis de reflexão, e pode haver outros.

Como sempre, no *Communiqué*, nós temos a possibilidade de fazer recomendações ou tópicos de importância, depois da apresentação sobre a implementação das emendas do contrato. As medidas e sua eficácia, eu acho que deve continuar a acompanhar isso com o GAC.

E como vemos do ALAC, então devemos esperar mais trabalho em política. E nos comentários públicos sobre as emendas, o GAC indicou que alguns temas deveriam ser mais elaborados. Então, eu estou aqui correndo, porque eu queria abrir o microfone para o público.

Bom, esses são alguns dos temas que foram incluídos na resposta às emendas do contrato. Em Kigali, fizemos algumas considerações sobre a preparação para a Próxima Rodada de Novos gTLDs.

Então, esses são elementos que poderiam entrar no *Communiqué*. Então temos oito minutos para sua consideração antes de passarmos à próxima sessão à Redação do *Communiqué*.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Há algum comentário, pergunta? Estados Unidos.

OWEN FLETCHER: Eu já mencionei, que há um relatório formal ou informal, eu acho que o Jeff mencionou a questão da métrica na plataforma OCTO. Eu mencionei antes, que as partes contratadas também querem informações e contribuições sobre o tema e o GAC poderia estar interessado também. A Comissão Europeia de Emma Carolillo, eu acho que nas sessões de ontem e hoje, houve grande interesse do GAC sobre o relatório do SSAC sobre o impacto das tecnologias emergentes no abuso do DNS. Eu acho que esse é um tema importante e também a proposta do ALAC, de trabalharmos juntos em temas de interesse mútuo, especialmente sobre os relatórios de domínios maliciosos. Eu acho que essa é uma preocupação comum entre o GAC e o ALAC.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Mais alguma pergunta?

SAMANEH TAJALIZADEHKHOOB: Muito obrigada por toda... Eu sou Sam, Diretora da Equipe de Pesquisas da ICANN Org. Eu estou liderando a Equipe do Projeto Métrica. E gostaria de convidá-los todos para a nossa sessão às 13h15 sobre Abuso do DNS, onde vamos falar das próximas passos. Infelizmente, nós teremos uma sessão de Redação do Communiqué, mas, claro, todos podem participar.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Agora, Reino Unido.

NIGEL HICKSON: Foi excelente esse diálogo. Eu sei que nós não teremos tempo para discutir esse novo tema. Mas, em outras reuniões, quando discutimos o RDRS, nós registramos os diálogos sobre vários minis PDPs ou micro PDPs sobre aspectos específicos do abuso do DNS. E, em geral, o GAC ficou interessado nisso. Eu acho que é algo que talvez devamos retornar a isso. Porque há questões específicas de alguns desses aspectos de abuso do DNS como *malware* e *phishing*.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Mais algum comentário? Bom, não estou vendo mais nenhuma pergunta. Então, pediria aqui na mesa se há algum comentário?

GEMMA CAROLILLO: Eu gostaria de agradecer a todos os delegados do GAC, que participaram da discussão. Então, eu sugeri um texto do Comunicado

que, bom, nós vamos levar em conta o que foi mencionado e escrever um pequeno texto para o *Communiqué*

Agradeço esse convite a Reg e eu, nós estamos disponíveis sobre qualquer pergunta sobre as ementas ou se isso vai ser um PDP ou não.

JEFF BEDSER: Eu gostaria de agradecer o convite e de falar para o GAC sobre o tema.

HIJAME ONGA: Muito obrigado. Foi a minha primeira reunião e eu fiquei muito impressionado.

MAHMUT ESAT YILDIRIM: Agradeço muito pela oportunidade de mostrar a nossa experiência para vocês. E espero... então estou disponível para compartilharmos informações e experiências aqui, em Colômbia. Só para lembrá-los que não sabem que o DNS, o abuso do DNS, eu acho que é o nosso objetivo estratégico número 4. E agradeço então a organização dessa sessão. Muito obrigado a todos. Essa reunião está encerrada. E voltamos às 13h15 para a reunião com o *Board*.

[FIM DA TRANSCRIÇÃO]