ICANN83 | Fórum de políticas – Discussão do GAC sobre atenuação do abuso de DNS
Terça-feira, 10 de junho de 2025 – 9h às 10h15 CEST

JULIA CHARVOLEN

Bom dia, bem-vindos à sessão do uso indevido do DNS. Essa sessão está sendo gravada e se rege pelos padrões de comportamento da ICANN. Durante a sessão, as perguntas e comentários serão lidas em voz alta, se estiverem no requadro dessa sessão, que inclui interpretação nos idiomas das Nações Unidas mais português. Se quiserem falar na sessão, levantem a mão em Zoom.

Quando mencionarem o seu nome, pode falar e, por favor, digam qual é o idioma em que vão falar se não for inglês, falem a uma velocidade razoável para a interpretação. E passo a palavra agora para o presidente do GAC, Sr. Nicolas Caballero.

NICO CABALLERO

Bom dia a todos. Obrigado, Julia. Damos as boas-vindas aos líderes do assunto, colegas nossos, Martin Kunc, Nick, da República Tcheca. Temos também os nossos colegas de Interisle Consulting Group. Temos Karen e Greg. Está Graeme Bunton, de NetBeacon, Susan Chalmers, dos Estados Unidos, e representantes do PSWG. Também contamos com o nosso representante Janos, da Comissão Europeia, e o Sr. Tomoromi Miyamoto, que representa o Japão.

Vamos ter uma conversa muito interessante sobre o uso indevido do DNS, e depois vamos passar a palavra para os presentes para poder ter uma conversa interessante. Então, passo a palavra para Tom.

TOMONORI MIYAMOTO Bom dia a todos, boa tarde, boa noite, a todos aqueles, os colegas que estiverem conectados em forma remota. Eu sou Tomonori, do Japão, Miyamoto, e apresento a agenda para a sessão. Depois da minha apresentação, vamos ter atualizações sobre o panorama do uso indevido do DNS e a sua mitigação, como teremos também uma apresentação do país anfitrião sobre campanhas de phishing, e uma apresentação de Interisle.

E depois vamos falar sobre processos de desenvolvimento de políticas dos PDPs e os próximos passos. Vamos nos focar em alguns PDPs, também na delegação dos novos gTLDspara o próximo ano. Nesse slide, vemos certa informação de contexto. Os contratos da ICANN, do RAA, precisam de que as partes contratadas, registros e registradores, adotem ações para a mitigação do uso indevido do DNS. E o meu país esteve trabalhando na definição do que é o uso indevido do DNS.

Dentro do contrato da ICANN, isso está limitado ao que é malware, botnet e phishing, farming e spam. A emenda de 2024 nesses contratos é um primeiro passo para considerar essa mitigação do uso indevido do DNS e considerar os próximos passos. Próximo slide. Alguns de vocês talvez estejam a par desse slide, esse gráfico.

Isso demonstra qual é o âmbito do contrato da ICANN que está representado no quadro verde. É limitado para poder lidar com o problema de forma efetiva.

Para isso, devemos considerar a relação que existe entre os registros e registradores. Também é possível procurar cooperação através da comunicação com o que está salientado no requadro em vermelho. Também estamos trabalhando com diferentes gTLDs da próxima rodada, mas é importante lembrar todo o panorama incluído nesse slide. Próximo slide, por favor.

Na nossa reunião de Seattle, fizemos uma apresentação sobre o que é a evidência e a situação do uso indevido do DNS. Na semana passada, tivemos diferentes seminários do GAC e uma apresentação sobre uma possível PDP. Além disso, a GNSO e seu equipo reduzido sobre o uso indevido do DNS apresentou seus prazos e objetivos, e a colaboração com esse grupo reduzido poderia ser uma forma de avanço. Próximo slide.

Essa é a última que eu vou mostrar. Ela não é 100% exata, mas mostra como é que são organizados alguns tópicos e discussões. À direita, vemos a mensuração no relatório do uso indevido, e mitigação aqui. Isso se baseia nos contratos da ICANN. Isso é feito para fins de transparência. E também é possível pensar em medidas que tenham a ver com uma transição. Podemos pensar em medidas proativas que incluam relatórios e outro tipo de atividades que se dêem no momento do registro.

Com base nos resultados do estudo INFERMAL, restringir os registros a granel poderia ser um ponto a considerar. A verificação seria um ponto a considerar. Agora vamos convidar Martin, de CZ NIC.

MARTIN KUNC

Estou aqui para compartilhar o nosso caso com relação ao phishing. Eu vou falar um pouco sobre os nossos projetos. Talvez já conheçam os mais importantes, como, por exemplo, Bird e as medições dos DNS que nós fazemos, denominadas ADAM, entre outras. Quem somos? CZ NIC é registro do domínio .cz, que também opera CSIRT.CZ.

E a história começa em junho de 2022, quando vimos alguns casos de phishing. No início, isso não era de muito interesse, mas em CZ começamos a nos encarregar disso porque não era algo usual. Nesse caso, o governo começou a dar subsídios para alguns cidadãos que estivessem em situações complexas, também, por exemplo, com relação a alguns personagens, algumas personagens, nesse caso, próximo slide.

Tínhamos algo como o BankID, isso não é muito comum em vários países, mas na República Tcheca os bancos se reúnem em algo que é chamado de BankID e utilizam as mesmas credenciais e são verificadas para poder acessar aos sites governamentais e também foram vítimas desse tipo de ato. Qual era o cenário, o palco, o cenário desse phishing?

As pessoas começaram a receber mensagens de texto, então lhes diziam que tinham certo dinheiro, certa quantidade de dinheiro. Foram enviadas bastantes mensagens, como podem ver. Eu sei que é difícil para vocês entender o que diz aqui, mas, basicamente, pediam que vocês fizessem clique, que clicassem em um determinado lugar. Isso levava para um site de phishing onde era pedido utilizar informação bancária e também outras questões, como, por exemplo, o tipo de autorização, autentificação, etc.

O interessante era que isso podia ser feito no horário comercial. Então, houve um exemplo, por exemplo, na República Tcheca, onde se perdiam algumas coisas e se podia ter acesso a um site. Nesse caso, isso não funcionava 24/7, mas durante o horário comum. Isso era assim porque os que estavam fazendo o delito usavam as credenciais em tempo real e precisavam da confirmação.

Aqui vemos um dos exemplos que se assemelha bastante com a exceção da URL. Aqui vemos outro exemplo. Nesse caso, pode-se escolher o banco. Nem sempre se podia escolher o banco, mas era necessário escolher entre alguns em particular. Aqui vemos a URL na parte superior. Havia um número, era necessário clicar, e assim podiam ver quão bem-sucedidos eram nessa campanha. Seguinte.

Aqui há outra visualização na tela seguinte. Bom, em 2022, começaram com 11 domínios por mês, o que não era muito comum. Não eram tão ruins. Em fevereiro de 2023, a quantidade aumentou, subiu para 72 nomes de domínio, que foi um aumento

importante para nós. Sabemos que, com o tempo, iriam melhorando, e nós também tínhamos que fazer também melhorar. Começamos a fazer uma busca ativa, estudar o processo e poder entender melhor os detalhes.

Entre os exemplos da pesquisa ativa, podemos ver essa zona e os domínios registrados. Então, em princípio, começamos utilizando caracteres similares utilizados para o site, mas porque tinham que modificar os nomes. Então, sempre surgiam novas ideias e nomes que não acabavam sendo de utilidade. Então, começavam se registrando diferentes nomes de domínio. Isso nos ajudou a ter ou criar uma lista de domínios, uma lista futura com domínios que sofriam de phishing.

Fazíamos uma verificação a cada cinco minutos e, em nenhum momento, o nosso endereço foi bloqueado. E assim que pudemos ver ou perceber quais os sites de phishing que estavam ativos, enviamos uma notificação e podemos atuar para poder bloqueá-lo em breve. Também podemos abreviar esse tempo para dar baixa a esses domínios. Próximo slide.

Então, estivemos considerando que fomos pesquisando e, assim, determinar o padrão. E havia alguns que emergiam depois, vários dias depois do registro. Primeiro o nome de domínio, depois o registro de DNS, depois os certificados. Então, quando isso já estava pronto, era habilitado o estado no diretório e se carregava o arquivo. E depois era analisado. Nós conseguimos analisar essas

amostras e vimos que, às vezes, diferiam e, às vezes, melhoravam. Próximo.

Caso tenham curiosidade, quero contar que os certificados são importantes para o tema da transparência. Tínhamos que considerar também as senhas, todas as sessões que tinham sido criadas e também outras questões que não são visíveis para nós com antecedência. Finalmente, consideramos que esse caso foi uma vitória, porque finalizou o mês depois de começar o ataque. 28 domínios foram registrados em março, se compararmos com o registro de 72 domínios em fevereiro.

Claro que há várias outras tentativas com outros TLDs e domínios simples, mas nada comparável com o que foi no começo. Seguinte slide. Esse gráfico aqui apresenta alguma dificuldade para entender, mas eu vou explicar. A cor verde representa as consultas que não foram resolvidas de forma correta. Neste caso, colocamos na cor verde porque são aquelas que não conseguimos resolver dentro dos domínios de phishing. Na cor preta, são aquelas que foram positivamente resolvidas.

É importante destacar que esse não é o número real de usuários, porque não vemos quantos usuários estão por trás de uma resolução única, mas dá uma ideia de para onde vamos e como é que estamos trabalhando. Seguinte slide, por favor. Neste gráfico, a comparação é muito mais positiva porque vemos que os traços verdes são maiores. Então, esta é uma espécie de vitória porque estamos vendo que estamos ganhando a luta.

O artigo 17 permite tirar os domínios das zonas que são suspeitosos ou que nós supomos que são favoráveis para a cibersegurança. O que nós fazemos é colocar um estado durante um mês e damos o nome de domínio, o titular do nome de domínio, que entre em contato e que diga o que está acontecendo, que diga, "olha, esse sou eu, isso não deveria estar acontecendo", enfim. Se fazemos alguma coisa que não está certa, podemos solucionar ou melhorar de tal forma.

E também publicamos uma lista de domínios os quais bloqueamos. Bom, isso seria tudo por minha parte. Espero que tenham aproveitado a minha apresentação e se tiverem perguntas, aqui estarei para responder.

TOMONORI MIYAMOTO Obrigado por compartilhar a experiência. Agora quero passar a palavra à audiência para as perguntas e respostas. Não sei se há algum comentário ou pergunta na sala.

GABRIEL ANDREWS Fala Gabriel Andrews para os registros. Muito obrigado pela apresentação, Martin. Eu fiquei muito interessado, realmente, e me impressiona quando falam desse tema de reconhecer que existem alguns domínios que são suspeitos e que estão sendo registrados, mas que ainda não vêm sinais de phishing, mas fazem igual o monitoramento e a verificação. Se eu entendi bem, é uma medida bastante proativa. Agora pergunto, vocês pensam que devem

esperar porque precisam de evidências mais concreta? Antes de tomar qualquer ação?

MARTIN KUNC Exatamente. Nós esperamos que apareça essa evidência para ter coisas mais específicas para poder tomar ou bloquear o nome de domínio e tomar algum tipo de ação quanto à investigação, por exemplo. O nosso processo está determinado de tal forma que se nós, por exemplo, vemos ou temos evidência podemos utilizar essa evidência para justificar um bloqueio, por exemplo.

GABRIEL ANDREWS Eu nunca vi uma conduta tão proativa. Realmente, se torna muito interessante. Eu sei que apresentou vários desafios em outros momentos, mas quando ainda não tem a evidência, muitas vezes isso é um desafio, mas vocês têm essas regras que permitem fazer um monitoramento e tomar iniciativa quando vocês suspeitam que o domínio será utilizado, por exemplo, para fazer phishing?

MARTIN KUNC Bom, isso foi feito durante uma campanha contra phishing para detectar aqueles nomes que poderiam ser utilizados para cometer phishing e ver ou analisar para ver se existem novos tipos de phishing.

ASHWIN SASONGKO SASTROSUBROTO: Fala Ashwin da Indonésia, para os registros. Muito obrigado aos oradores pelas apresentações. Eu quero dizer várias coisas. Quão efetivo é o uso das DNSSEC como medida de segurança em um website e também quão efetivo é o uso de uma certificação de segurança. Isso presta para mitigar o uso indevido do DNS ou não é suficiente? E quanto ao que falou o segundo orador de CZ. O senhor dá vários casos de phishing. Em todos eles, se utiliza o ccTLD .cz ou também utiliza o gTLD? Muito obrigado.

MARTIN KUNC: Eu não sei se posso responder à primeira pergunta, mas quanto à segunda parte. No caso, esta pesquisa se tomou como base o espaço .cz e aí facilitou o nosso trabalho. Mas também sabemos que trabalhamos com outros domínios, mas não foi da mesma magnitude.

ASHWIN SASONGKO SASTROSUBROTO: No website da ICANN, por exemplo, quanto à minha primeira pergunta, sempre falam que devemos ativar a DNSSEC. Quão efetiva é esta operação para evitar o uso indevido do DNS? Na Indonésia, igual que em muitos outros países, trabalhamos com uma norma ISO 27000, que tem a ver com padrões para gerenciamento de sistemas de segurança. Então, 27001 da ISO. Eu gostaria de saber quão efetiva é.

MARTIN KUNC

Bom, nas DNSSEC não ajudam para nada a combater o phishing. E com respeito à norma ISO 27001, eu não sou a pessoa indicada para responder esta pergunta porque está fora do meu alcance. Eu peço desculpas.

TOMONORI MIYAMOTO

Mais alguém está solicitando a palavra. Aderonke, desculpe se a pronúncia está errada.

ADERONKE ADENIYI

Obrigada, Martin. As apresentações foram muito boas. Para os registros, eu sou Aderonke, da Nigéria. Com respeito ao BankID, essa identificação bancária, o senhor considerou trabalhar com o regulador bancário para mitigar o uso indevido do DNS? Na Nigéria temos o número de verificação bancária, que é utilizada em todas as plataformas de serviços digitais. Queria saber se, em algum ponto, trabalhou o senhor junto com a entidade reguladora do setor bancário para emitir essa identificação bancária, esse BankID.

MARTIN KUNC

Não tivemos muito sucesso quando tentamos entrar em contato com a entidade de regulação. Mas, felizmente, eles assumiram o assunto e começaram a trabalhar com seus usuários, começaram a trabalhar contra as tentativas de phishing, enviando notificações aos usuários e tal. Isso funcionou bem. Fizeram o todo possível.

TOMONORI MIYAMOTO Bom, agora convidaremos a Karen e o Greg, que vão fazer a sua apresentação sobre phishing no uso indevido do DNS.

KAREN ROSE Obrigada. Estou aqui junto ao Greg Aaron. Somos da Interisle Consulting Group. Nós temos mais de 20 anos de experiência de expertise nesta área de trabalho. Estamos fazendo pesquisas de diferentes usos indevidos de recursos da internet e crimes cometidos. No dia de hoje, especificamente, vamos falar sobre o uso indevido do DNS através do phishing.

Verão que nós publicamos um relatório que abrange muitos outros exemplos e casos. Temos pouco tempo, então serei breve. Próximo slide. Concluindo, infelizmente, o phishing e o uso indevido do DNS estão crescendo a ritmos alarmantes. Com mais de dois milhões de ataques do uso indevido e mais de um milhão e meio de domínios foram atacados nos últimos 12 meses. Esta situação subestima o problema em grande escala porque há muitos ataques que simplesmente não são informados.

77% dos casos, esses domínios foram registrados especificamente para cometer um ciberataque. E o phishing afeta muito a sociedade e é muito caro porque calculamos que por minuto dedicam-se mais de 18 mil dólares em perdas financeiras para solucionar todos esses problemas. E lembremos que, à escala global, muitos dos casos não são informados.

Temos também que reconhecer que estas iniciativas para combater o uso indevido do DNS, até hoje, não foram efetivas, em grande parte, ou em grande medida. Aqui vemos um quadro de uma empresa chamada Freenum. E esta empresa combateu o phishing por um tempo, mas vemos que depois desses ataques de phishing começaram de novo e houve como um rebote no ataque. Aqueles que cometem o phishing exploram-se e aproveitam de duas coisas, preços baixos e facilidade no registro.

Quando um domínio tem um preço de dois dólares ou menos, isso facilita a atividade de phishing. E aqueles que cometem os crimes se aproveitam dessa situação. Vemos a participação de mercado dos novos gTLDs, aqui no quadro, que é apenas de 11% na cor amarela. Agora, no outro quadro, vemos que os novos gTLDs representam 51% dos ataques de phishing no último ano.

Então, isso significa que este tipo de domínio continua sendo atraente para os perpetradores de ataques de phishing. .com, .net, por exemplo, .org, são utilizados para promoções gratuitas e para alguns combos de promoções de diferentes produtos. Também aqueles que cometem phishing aproveitam a facilidade de registro de um domínio com poucos requisitos, sem verificação de identidade, sem validação de dados, e preferem também algum tipo de fornecedor, que são registradores e TLDs que estão nesse ponto intermédio entre ser econômicos e de fácil registro.

Isso sempre está dentro dos primeiros registradores, nos primeiros 10 ou 5, que se utilizam cada vez durante um ano. Próximo slide.

Aqueles que atacam registram nomes de forma surpreendente, e é fácil de entender, de identificá-los, porque cumprem alguns padrões. E aqui apresento alguns exemplos de alguns ataques. Nomes gerados por algoritmos que são variações de um tema, assunto ou cadeias de caracteres totalmente aleatórias.

Também há nomes que se assemelham muito a marcas comerciais e também utilizam os mesmos dados de registração uma e outra vez. E também geram informação de registração que é falsa. Então, temos que detectar esses padrões. Alguns ccTLDs já têm sistemas no DNS para detectar esses padrões e também temos algumas ferramentas comerciais que permitem validar endereços.

GREG AARON

Cada ano, estudamos como se registram esses domínios. Os atacantes não registram um ou dois domínios por vez, mas registram um grande número de domínios e, como disse Karen, cumprem um padrão. E isso faz com que sejam fáceis de detectar. Se vemos que há um domínio registrado, depois outro e outro com o mesmo registrador, veremos que geralmente serão utilizados para phishing.

37% desses domínios como média utilizados para phishing se registram de forma massiva, por lote ou pacote, digamos. Mesmo que nem sempre esses lotes ou pacotes podemos encontrar um domínio utilizado para phishing, mas esses conjuntos ou pacotes de domínios às vezes têm muitos registros, domínios registrados,

como por exemplo o de 17 mil, registrados por um único cibercriminal ou atacante.

Esses atacantes agora avançam com rapidez e a vítima fica presa desse ciberataque de forma imediata, em menos de oito horas depois de ter sido registrado o domínio. Esses atacantes sabem que o domínio será suspenso depois, mas trabalham de uma forma tal que permite continuar cometendo crimes num domínio e em outro, e em outro, e enquanto possível vão continuar avançando. Vemos muitos phishing, por quê? Porque é bem-sucedido para aqueles que cometem esse crime, mas temos que pensar por que está acontecendo isso e por que temos essa geração constante de domínios.

KAREN ROSE

O uso indevido do DNS é possível graças às eleições, opções que tomam a ICANN, que tem a ver com como funciona o mercado. E escolhas que tomam as empresas para levar adiante os seus negócios. Nós sempre dizemos que a concorrência é boa, então ter mais concorrência seria melhor ainda, embora de uma perspectiva econômica isso nem sempre é assim.

Muita concorrência sem as regras correspondentes pode ter efeitos negativos, então é como se tivéssemos uma indústria que gera poluição e que gera muitos custos na sociedade e nos consumidores. O mercado do DNS é muito competitivo, hoje temos mais de dois mil registradores, centenas de TLDs abertos, e os

nomes e domínios são como commodities, produtos básicos se podem trocar entre si e tem um custo marginal zero.

Então, se não temos uma política efetiva contra o uso indevido, os criminosos se aproveitam dessas possibilidades e da dinâmica do mercado. Nós acreditamos que precisamos de medidas razoáveis, proativas, para prevenir o uso indevido do DNS e não só mitigar o prejuízo quando é feito, embora também sempre seria de utilidade ter uma mitigação mais eficiente. Temos que fazê-lo agora, implementar essas políticas agora, porque na medida em que se adicionem novos gTLDs ao mercado, isso irá gerar muita mais pressão e também vai gerar uma pressão competitiva maior no mercado. E também vai afetar os preços. Próximo slide.

GREG AARON

Estamos vendo uma tendência, principalmente na Europa. Os operadores de registro estão inovando. Por exemplo, em alguns casos, não pedem a todos os registratários que demonstrem a sua identidade, mas seguem abordagens que envolvem risco. Por exemplo, alguns operadores de registro dizem os registros maciços são um exemplo de um risco. Não sabemos quem é o registratário, mas está registrando muitíssimos domínios.

Nesse caso, sim, poderíamos pedir que verifique a sua identidade e talvez não deveríamos permitir que esses domínios funcionem até que estejamos tranquilos e saibamos quem é que está registrando. E isso está acontecendo em alguns TLDs da Europa. A

ICANN tem requisitos de verificação que são praticamente mínimos.

De fato, uma das iniciativas de cumprimento contratual da ICANN, descobriu que em 20% dos casos não eram seguidos os passos mínimos de validação. Então, nós vemos aqui uma oportunidade que é estudar essas abordagens com base em riscos para justamente prevenir e, assim, dificultar o agir dos delinquentes.

Nós temos essas ideias, fortalecer os requisitos de verificação, ver o que se passa com esses registros maciços. Isso vai de mãos dadas, se relaciona estreitamente. Talvez vocês não saibam que nos contratos da ICANN é necessário que os operadores de registro trabalhem com todos os registradores acreditados pela ICANN. Isso tem vários motivos. Por exemplo, que as regras de jogos sejam iguais para todas as empresas que participam.

Mas alguns registros exigem que trabalhem com registradores que até hoje trazem alguns negócios que não são benéficos, que são prejudiciais, porque tem registratários que talvez não sejam bons atores. Então, aí tem trabalho pela frente. Os registros têm ferramentas para detectar o uso indevido antes de que aconteça e poder agir. Quer dizer que há algumas soluções. Ou seja, aqui em resumo, queremos que saibam que existem ferramentas que podem ser utilizadas e políticas que poderiam melhorar essa situação.

KAREN ROSE

Temos um relatório que vai ser publicado no terceiro trimestre desse ano. Fiquem atentos a essa publicação. Nós, nos nossos relatórios, não só estudamos nome de domínio, mas também subdomínios, hospedagem, web, phishing, malware, entre outras. Por isso é que convidamos a que visitem o nosso website e ler os nossos relatórios.

Nós temos a nossa própria web, que se chama cybercrimeinfoserver.org. Aí temos muitíssimos dados, tabelas de classificação, listas. Também estamos em Substack. A cada vez publicamos blogs. E, logicamente, temos o nosso website na tela, e com muito prazer podemos entrar em contato com vocês através do e-mail. Obrigada pela atenção.

TOMONORI MIYAMOTO

Obrigado, Karen e Greg pela sua intervenção. Vou passar a palavra para o Janos.

JANOS DRIENYOVSZKI

Obrigado, Tomo. Vamos passar para os próximos passos em desenvolvimento de políticas e aos processos de políticas ou micro-PDPs que poderiam ser desenvolvidos. E depois, ou antes, vou passar a palavra para o Graeme, para que faça a sua apresentação.

GRAEME BUNTON

Fala Graeme Bunton, sou diretor Executivo de NetBeacon. Faz umas duas semanas publicamos um documento branco onde

propomos cinco possíveis ideias sobre PDPs. Hoje não há tempo para isso, para os detalhes, mas vou colocar o link para essa informação. É um documento de 22 páginas para ler, mas eu vou fazer um comentário breve sobre ele.

Agora, por que que trabalhamos com esse assunto? NetBeacon trabalha e dedica muito tempo a pensar como reduzir o uso indevido do DNS. E também somos uma parte contratada. Então, trabalhamos de forma muito similar ao que faz o Interisle. Temos um projeto para poder mensurar e entender o uso indevido do DNS. Isso é chamado de NetBeacon Map, ou mapa de NetBeacon.

E considerando esses dados, queremos ver se podemos dar apoio aos debates que se dão na comunidade com algumas ideias que pensamos poderiam ser alcançáveis em tempo adequado e que teriam impacto nas questões de uso indevido do DNS. Talvez poderíamos pensar em ter PDPs que fossem mais limitados quanto ao alcance ou escopo para a comunidade. Vou ser breve, não vou dar detalhes, mas vai haver uma obrigação para que o registro se informe sobre o uso indevido do DNS. Vão receber um relatório de uso indevido do DNS e se deve agir quando está essa evidência.

Próximo slide. APIs. Bom, um dos pontos mais importantes do relatório INFERMAL, e parabéns à equipe da OCTO pela realização desse relatório, tem a ver com que os APIs que não têm acesso têm uma possibilidade de 401% de sofrer abuso. Então, é importante que os registradores tenham acesso a esse tipo de ferramenta para poder controlar essas condutas de registro.

Os contatos para uso indevido de subdomínios podem ser aplicados a esses subdomínios que são utilizados por terceiros. Mecanismos de recursos para o registratário, quando há registros de registratários que trabalham de forma diligente para lutar contra o uso indevido do DNS à escala, podem se fazer erros. Os registratários, às vezes, podem estar impactados pela mitigação desse uso indevido.

Para isso, tem que ter ferramentas para poder resolvê-lo. Coordenação DGA e botnets. Temos os algoritmos de registro de nomes de domínio que, muitas vezes, não funcionam de forma eficiente. Então, aqui propomos uma função centralizada para que a ICANN colete essa informação e a espalhe, e que seja mais eficiente no momento de fazer a disrupção dos botnets.

Posso falar sobre cada um desses PDPs, posso usar todo o tempo que vocês quiserem, talvez nos corredores, mas algumas mensagens-chave que quero que hoje levem com vocês. Essa é uma oportunidade concreta de avançar nessa comunidade em relação aos PDPs, desenvolvimento de políticas, para marcar a diferença no que é o uso indevido do DNS.

Mas temos que estar todos comprometidos, empolgados de forma coletiva para ter um processo que seja delimitado e tenha um escopo, isso é necessário, isso vai requerer de um foco, e também o progresso em tempo vai precisar de que o foco seja muito específico, intenso. Isso se torna complexo na medida em que

aprofundamos nos detalhes, e também tem um impacto operacional, porque há questões que devem ser resolvidas.

Mas se podemos fazer a diferença, podemos ter ou dar passos positivos, isso é melhor do que não fazer nada. O tamanho do que acontece tem muito a ver com o tamanho do que podemos fazer. E a última parte que eu quero enfatizar em relação ao caminho, os padrões que se vê no uso indevido do DNS, temos que passar desse relatório de uso indevido individuais para abordar o uso indevido do DNS à escala.

Nos nossos dados vemos registros e registradores que acabam suspendendo nomes de domínios que são maliciosos, mas a obrigação está também no nível do relatório individual do uso indevido, e também na restrição dos registros maciços. Temos que chegar a um ponto no qual possamos abordar o uso indevido do DNS, não só em nível individual, mas também quando há campanhas que representam o uso indevido.

E acho que essas são as novas ideias que a comunidade deve começar a abordar. Da nossa perspectiva, nós publicamos esse documento, acho que conseguimos, alcançamos o nosso objetivo, falamos em ideias que podem ser bem-sucedidas, e se não são essas, estão bastante focadas, e é o que gostaríamos de continuar vendo na nossa comunidade, que a comunidade continue falando e avançando nessa direção. Obrigado a todos pela oportunidade de ter a palavra.

NICO CABALLERO Muito obrigado. Antes de passar a palavra para Tomo, eu queria pedir aos nossos representantes do GAC que considerem a necessidade de agir. Sabemos que os criminosos estão nos olhando atualmente, e desenvolver um PDP que leve cinco anos, bom, vai colocá-los uns passos para frente de nós. Acho que deveríamos tomar ação rapidamente.

JANOS DRIENYOVSZKI Vamos agora nos centrar naquilo que o GAC deveria fazer. Eu gostaria de falar primeiro da ideia apresentada na Câmara de Partes Contratada numa reunião do dia de ontem que é beneficiosa para a discussão. Uma das ideias era solicitar os requisitos de ter um relatório do que são os domínios registrados de forma maliciosa.

A segunda ideia tinha a ver com uma possível emenda contratual ou adenda para garantir que os registradores possam oferecer o programa de revendedor para ter as medidas contratuais necessárias caso tenham que usar contra o uso indevido do DNS. Outra ideia era o desenvolvimento de um quadro normativo regulatório para todos os operadores de registro de gTLDs e a quarta ideia era desenvolver melhores práticas para melhorar a qualidade dos relatórios.

Também foi mencionada a palavra ou termo medida proativa e registros massivos. Atualmente, nos encontramos explorando o

terreno destas medidas proativas e também medidas reativas ou reagentes. A ideia seria conseguir coisas significativas antes da próxima rodada. Eu acho que deveríamos priorizar algumas ações específicas nesse sentido. Isso também tem a ver com o que falamos antes sobre esses PDPs mais resumidos.

No comunicado, o GAC indicou a importância de analisar o ponto das registrações ou registros massivos dos nomes de domínio. Claro que esses registros massivos, como falaram hoje de manhã, apresentam um alto risco de ter relação com o uso indevido do DNS e também o seu impacto é maior do que se registra um nome a nível individual.

Talvez políticas de registração mais estritas e medidas proativas poderiam, sem dúvidas, melhorar esta situação. Agora, com respeito às partes contratadas, uma ideia seria implementar medidas proativas quanto à registração massiva. Isso poderia restringir os registros massivos de apps, por exemplo, restringindo o acesso a esse tal app ou também fazendo uma verificação daquele que registra e pensamos que esta ideia é bastante realista.

Poderia ser exigido maior preço para esses registros massivos e essas medidas proativas poderiam, de alguma forma, complementar as medidas reagentes e as medidas de mitigação que as partes contratadas apresentaram. Também NetBeacon propôs trabalhar e verificar os domínios associados. Então, eu acho que temos aqui uma combinação de medidas proativas e reagentes.

Falando em outras medidas proativas e de mitigação, no comunicado de Hamburgo, o GAC reiterou a importância do monitoramento proativo e também foi mencionada a necessidade de práticas para detectar o uso indivíduo do DNS e o trabalho sobre os dados de registração dos nomes de domínio, o GAC encoraja registradores a que explorem o uso de sistemas de ação de uso indivíduo do DNS com base no API.

Isso poderia também significar identificar indicadores de registro massivo no momento do início, e essa medida estaria em linha com a Recomendação 1 que fez a equipe reduzida sobre o uso indivíduo do DNS do Conselho da GNSO no mês de outubro de 2022. Isso quer dizer que todos os registros que apresentem algum nível de risco deveriam estar submetidos a alguma verificação.

Também temos exemplos de medidas proativas sobre os ccTLDs da Europa que têm a chance de implementar esses sistemas de detecção e implementação através do AI. Também se falou do ciclo de vida do nome de domínio e de fazer verificações correspondentes. Agora vou passar a palavra à minha colega Susan.

SUSAN CHALMERS Obrigada, Janos. Eu vou falar sobre uma terceira ideia que foi debatida pelos líderes do tema dentro do GAC, que tem a ver com as obrigações de preparar relatórios. É importante considerar de poder contribuir a esse relatório e as medições ou métricas. O

Instituto NetBeacon oferece algumas métricas ou medições. Nós também trabalhamos em diferentes relatórios.

Por exemplo, no Interisle temos também o relatório do INFERMAL, que foi debatido amplamente na reunião ICANN82. Todos esses documentos são muito relevantes. O Departamento de Cumprimento Contratual da ICANN também oferece relatórios mensais sobre o uso indevido do DNS, que representa uma evidência muito interessante.

E também sabemos que as partes contratadas implementaram as obrigações sobre o uso indevido do DNS em 2024. Mas não há requisitos para as partes contratadas para que publicamente emitam relatórios sobre as atividades de mitigação do uso indevido do DNS ou implementação correspondente das emendas ou adendas. Então, poderíamos nos centrar nas estatísticas desses relatórios.

Outra sugestão que tem a ver com as ideias já escutadas no dia de ontem, próximo slide, por favor são as seguintes. Temos as próximas etapas ou passos a cumprir, que são os diferentes caminhos quanto às políticas. Se participaram do seminário oferecido anteriormente para a reunião de ICANN83, devem saber já que há uma equipe reduzida da GNSO que está trabalhando no uso indevido do DNS.

Este grupo tem como objetivo avaliar os esforços de mitigação do uso indevido DNS, redigir algumas recomendações para o mês de setembro deste ano e realizar um relatório final no mês de outubro,

apresentar um relatório final. Sabemos que este prazo talvez deva ser limitado. E o que eu gostaria é que os membros do GAC saibam que esse grupo está trabalhando junto com a GNSO.

Na reunião que a gente vai manter com o board no dia de hoje, vou pedir que o staff apresente aqui as perguntas que vamos propor ao board. E vamos discutir com a diretoria o seguinte. Talvez muitos concordem que os PDPs deveriam se realizar num prazo mais reduzido, porque os PDPs levam anos.

A pergunta que vamos apresentar à diretoria, isso não é específico do uso indevido do DNS, mas perguntamos como poderíamos começar a mudar algumas etapas no processo dos PDPs para que os resultados sejam apresentados ou consigamos obter resultados mais rapidamente, não em três anos ou três anos e meio, mas talvez num período de 12 meses ou ainda menos.

Então, eu convido os representantes do GAC a que considerem também esta linha de trabalho. Muitos representantes do GAC estão familiarizados sobre como podem participar e como também realizar mudanças nas políticas dentro da ICANN. Há diferentes processos de desenvolvimento de políticas. Estão os processos de desenvolvimento de políticas ou processos multissetoriais que exigem a participação de todas as partes da comunidade da ICANN, inclusive o GAC.

Os PDPs, por sua vez, dão como resultado uma política de consenso e essa política de consenso termina sendo parte dos contratos vinculantes para todas as partes. Outra linha de trabalho

poderia ser fazer mudanças nessas políticas, talvez realizar emendas aos contratos realizados entre a ICANN, registradores e registratários. E, por enquanto, os contratos são negociados numa base bilateral.

Em 2024, foram realizadas algumas emendas que começaram a ser implementadas e que estabelecem novas obrigações para os registros e registradores, mas são resultado de, basicamente, negociações bilaterais. A diferença dos PDPs, as partes interessadas que não são ICANN ou partes contratadas não estão envolvidas nesse processo.

Para aqueles representantes do GAC, a ferramenta fundamental é a recomendação do GAC, com isso podem gerar uma recomendação consensuada que depois será analisada pela diretoria e, dessa forma, o GAC pode efetuar mudanças nas políticas. Esta é a ferramenta que tem o GAC, especialmente para aqueles representantes que são novos no comitê. Seguinte slide.

Temos 15 minutos, sim? Estou certa? Queremos que fique tempo para o debate dentro do GAC. Por sua vez, o presidente lançou uma convocação para tratar temas antes da reunião ICANN83. Esta equipe também ofereceu algum documento à lista do GAC antes da reunião e aqui, o que eu fiz foi simplesmente mencionar os pontos principais do que disponibilizamos quanto aos temas de importância.

Vemos dentro deles o que tem a ver com o uso indevido do DNS. Também sugerimos a revisão do panorama do uso indevido do

DNS e a sua mitigação, alguns pontos referidos aos PDPs e os próximos passos ou etapas a cumprir. E também sugerimos a criação de PDPs que sejam mais centradas ou mais limitadas para poder conseguir resultados consensuados em prazos mais curtos. Isso é o que nós queremos apresentar para vocês e passar a palavra também para que realizem os seus próprios comentários.

NICO CABALLERO

Obrigado, representante dos Estados Unidos. Quero voltar ao slide número 12. Está, sim, muito bem. Está aqui na tela. Antes de passar a palavra à Indonésia, peço desculpas, porque continuo esperando a Ashwin. Este é um novo pedido de palavra. Vejo que sua mão está levantada no Zoom.

Antes de passar a palavra, então, e de que todos possam realizar as suas perguntas ou comentários, quero destacar o seguinte. O processo de desenvolvimento de políticas é importante e é importante que os membros do GAC participem. Queremos que se sintam à vontade, que tenham a oportunidade de participar de forma significativa, que se sintam à vontade, já disse.

Ou seja, quero manifestar o seguinte. Para que serviria, de que utilidade seria participar de um processo de desenvolvimento de políticas se não temos a oportunidade de apresentar as nossas perspectivas, de fazer que nossa voz seja escutada. E vou dar apenas um exemplo. Se a presidência não é eficiente, as suas ideias, então, não serão compartilhadas, porque vão passar a

palavra a outra pessoa antes de que vocês possam manifestar as suas próprias perspectivas dentro desses PDPs.

Então, como já disse, a ideia seria que vocês se sintam à vontade participando nesses PDPs. E claro que estou totalmente de acordo com o que disse a representante dos Estados Unidos, ou seja, ter processos de desenvolvimento de políticas mais efetivos e breves. De uma perspectiva governamental, não podemos permitir dois, três ou quatro anos ou mais até chegar a uma solução.

Não é necessário que eu explique os períodos de gestão, de gerenciamento governamentais. Em alguns países, o período de presidência é de quatro anos. Os ministros das relações exteriores, talvez, estão na sua gestão durante dois anos. Também os de tecnologia da informação e a comunicação. Ou seja, isso depende de cada país. Mas, enfim, vocês entendem o que eu quero dizer ou comunicar. Agora, tem a palavra o representante da Indonésia.

ASHWIN SASONGKO SASTROSUBROTO: Obrigado, Nico. Tenho uma pergunta com relação à norma ISO 27001. É suficientemente robusta para evitar, prevenir o uso indevido do DNS na sua experiência? E pergunto ao colega da República Tcheca. Na Indonésia, temos um problema muito grave atualmente. E também a Indonésia é membro da ISOIC, que tem um comitê, um subcomitê 27 que se dedica especificamente à cibersegurança, e outro comitê encarregado das TICs.

Se essa norma, então, não é suficiente ou suficientemente robusta, temos que dizer para a organização que faz as normas ISO, a Organização Internacional de Normalização, nós teremos uma reunião daqui a pouco com eles. Então, queremos ver isso, porque a ideia é fazer uma política na qual se utilize essa norma ISO 27001 para proteger os nossos sistemas. Então, se desde a experiência da ICANN essa norma não é suficientemente robusta, temos que dizer isso para a Organização de Normalização. Temos que falar isso com eles. Muito obrigado.

NICO CABALLERO Obrigado, Indonésia. Tomamos nota do seu comentário agora. Toma a palavra a representante da Índia.

SUSHIL PAL Obrigado, Sr. Presidente. Obrigado, Interisle e a NetBeacon, especialmente pelas suas apresentações e também por essa proposta de fazer PDPs que sejam mais limitados. Insisto em que estamos vendo sintomas e não a causa dessa situação. Estamos falando na correlação entre os registros maciços e os custos baixos e os atores maliciosos.

Mas, na minha opinião, esses são os sintomas e não a causa. A causa está nas políticas, dados e na identificação. Nós vivemos num mundo físico, mas, nesse mundo, nós sabemos quem vive na nossa mesma vizinhança, não é? Mas, no mundo digital, há anonimato. Não sabemos quem são os atores maliciosos. Então,

eles têm o caminho livre para agir, e o único que resta é dar baixa a um domínio.

Então, não acho que aumentar o custo de 2 dólares para 10 dólares para registrar um domínio tenha como consequência uma menor quantidade de domínios maliciosos, porque os benefícios para esses atores maliciosos são enormes, vimos na apresentação. Então, eu acho que o que precisamos é que não só os registradores, mas também os registratários sejam responsáveis e prestem contas, e também haverá um custo adicional para registradores e registratários. Temos que ver essa solução. Obrigado.

NICO CABALLERO Muito obrigada, Índia, pela participação. Estão faltando sete minutos e temos sete pessoas que solicitam a palavra. Então, peço, por favor, que sejam breves. Susan, quer adicionar mais alguma coisa antes de começar com as perguntas? Bom, então, passo a palavra para a Comissão Europeia.

GEMMA CAROLILLO Fala Gemma Carolillo, da Comissão Europeia. Muito obrigada aos colegas do GAC por ter organizado essa sessão que foi tão informativa e obrigada aos oradores também. Com relação ao que vamos considerar no comunicado, quero dizer o seguinte, nós vemos algo muito bom nessa situação, vemos que há um impulso, um ímpeto na comunidade para avançar no uso indevido do DNS depois das emendas contratuais.

Vemos que as partes contratadas tiveram iniciativas, escutamos a NetBeacon, vimos os estudos de Interisle, vemos muito ímpeto e devemos aproveitá-lo e colaborar com os outros grupos da comunidade. A prioridade para o GAC sempre foi obter medidas antes de uma próxima rodada, com o qual devemos ser pragmáticos e poder alcançar medidas concretizáveis no prazo disponível. Isso significa ter prioridade, sem esquecer o panorama geral, mas temos que priorizar.

Então, pensamos que é importante emitir um assessoramento com relação a ter PDPs que sejam mais limitados, específicos, e ao mesmo tempo sugeriríamos que fizéssemos essa lista de prioridades ou identificar temas prioritários. Nós escutamos sobre medidas proativas, padrões de comportamento que devem ser monitorizados, vimos o tema dos registros maciços, se fizeram propostas diferentes, com o qual, além disso tudo, consideramos que é importante considerar as obrigações em matéria de transparência, que foi parte de um comentário público feito pelo GAC com relação às emendas contratuais sobre uso indevido do DNS.

NICO CABALLERO

Obrigado, Comissão Europeia. Tenho agora seis sessões para falar no comunicado, então vai ser considerado. Toma a palavra o representante do Canadá.

IAN SHELDON

Obrigado, Nico, vou ser breve, porque outras pessoas querem falar também. Obrigado. Obrigado pelo relatório de NetBeacon. Concordo com você que o melhor é o inimigo do bom e que devemos avançar, então estou de acordo também com o tema dos PDPs sem ser oportunos.

Quero convidar o GAC a que leia o relatório de NetBeacon, que está muito bem redigido, não é excessivamente técnico e tem boas sugestões. Obrigado. E vou participar das discussões do GAC para ver como continuamos perante esses PDP.

NICO CABALLERO

Obrigado. Tem a palavra, Países Baixos.

MARCO HOGEWONING

Obrigado, Nico. Sou Marco, de Países Baixos. Eu quero me unir aos agradecimentos pela organização dessa sessão. Como disse o colega, temos que ser conscientes de que o perfeito é inimigo do bom. Temos que avançar e acho que está na hora de ver as opções que temos pela frente. Temos que trabalhar com a GNSO e a diretoria e talvez possamos achar um ou dois assuntos para continuar trabalhando perante a próxima reunião.

JORGE CANCIO

Obrigado, Nico. Sou Jorge Cancio, da Suíça para os registros. Eu me uno aos participantes anteriores. É importante ver o que é que falamos com a GNSO e com a diretoria e ver como continuamos. De qualquer forma, acho que há potencial nessa ideia de ter processos

de desenvolvimento de políticas mais limitadas, específicas, e talvez quero corrigir a Susan. Eu não acho que se tenha dado um PDP que tenha demorado menos de um ano, mas é claro que posso errar.

NICO CABALLERO Obrigado, esperamos que isso possa ser modificado. Agora tem a palavra o representante da Dinamarca.

FINN PETERSEN Obrigado, senhor presidente. Sou representante da Dinamarca para registros. Obrigado pela apresentação. Agradeço essa apresentação. Estou de acordo em ter PDPs mais limitados e gostaríamos de que se concretizasse antes do lançamento da próxima rodada. Queremos ver medidas proativas e acho que o registro maciço é um exemplo, gostaríamos de ver obrigações em termos de identificação, de identidade, ou diferente tipo de validação, dados de contato, talvez precisemos disso hoje em dia.

Também falta transparência na hora de priorizar antes da próxima rodada. Consideramos que se devem ter medidas proativas, isso será apenas um passo para frente, onde quer que estejamos indo. Com relação a registros maciços, na sua análise, definiram qual o limite de registros para considerar uma registração maciça? Obrigado.

GRAEME BUNTON

Fala Graeme, de NetBeacon para os registros. Com relação aos registros maciços, quando tentamos colocar um limite específico de domínios, os atores maliciosos o que vão fazer. Vão por cima ou por baixo desse número. E isso tem um impacto no mercado. Na busca, podemos adicionar X quantidade de domínios, então, isso vai ter impacto. E aí temos um impacto no mercado.

É por isso que é de muito risco colocar um limite ou uma quantidade limitada determinada a um registro maciço. Nós usamos o relatório INFERMAL, trabalhamos com o API para ter uma ferramenta. Em lugar de ver essa abordagem, nós trabalhamos com essa ferramenta que achamos ser mais efetiva.

Em segundo lugar, temos que ver a verificação de nomes de domínio associados. Isso é reativo, mas se um registrador tem que ver todos os domínios na conta de um dos seus clientes, que podem ser 10, 20 ou 100 domínios, isso é oneroso para o registrador. Então, eles vão ser mais cuidadosos nos registros, porque vão ter essa obrigação de verificar todos esses domínios. E esperamos que isso tenha um impacto no mercado, incentive o comportamento certo. Por isso, colocamos essa proposta no nosso relatório.

NICO CABALLERO

Obrigado. Temos que dar por encerrada essa sessão. Realmente é muito positivo ver que há consenso nas nossas sessões, porque no contexto internacional atual, o consenso não é algo que se dê tanto. Vemos que há consenso nos três temas de importância. Não

vou ler novamente. Susan quer falar para encerrar, porque ela lidera esse assunto.

SUSAN CHALMERS Muito obrigada, Sr. Presidente. Da perspectiva dos Estados Unidos, os prazos dos PDPs devem ser reduzidos de forma significativa para concretizar políticas -- o DNS como resultado da próxima rodada de novos gTLDs. Isso vai dirigido à comunidade da ICANN em geral.

Escutamos propostas da Câmara de Partes Contratadas, o NetBeacon, número de Partes Contratadas Comerciais Interessadas também, o Comitê At-Large também, o Grupo de Partes Interessadas Não Comerciais também. Tem prioridades que têm a ver com as políticas sobre uso indevido do DNS.

Vemos que estamos avançando numa direção conjunta e que a comunidade multissetorial da ICANN deveria trabalhar em conjunto para obter um resultado sobre esse assunto. Esse momento é muito importante para que sejam geradas políticas dentro desse contexto.

NICO CABALLERO Obrigado. Estamos superando o tempo permitido. Depois da pausa, vamos ter uma sessão conjunta com a ALAC e desfrutem muito do café.

[FIM DA TRANSCRIÇÃO]