PT

ICANN82 | Fórum da Comunidade – GAC: discussão sobre abuso de DNS
Terça-feira, 11 de março de 2025 – 10h30 às 12h PST

NÃO IDENTIFICADO — Bom dia a todos. Peço que tomem seus assentos. Vamos começar.

GULTEN TEPE OKSUZOGLU — Olá e bem vindos à discussão do GAC e ALAC sobre mitigação do abuso do DNS. Essa sessão está sendo gravada e é regida pelas normas de comportamento da ICANN e anti-assédio.

Durante essa sessão as perguntas e comentários só serão lidos se colocados no formato correto. Diga o nome e o idioma que vai falar se não for em inglês, fale de forma clara e devagar para uma boa interpretação. E não esqueça de silenciar todos os dispositivos ao falar. Todas as funcionalidades dessa sessão estão na barra de ferramentas do Zoom. Com isso eu passo a palavra ao presidente do GAC, Nicolas Caballero.

NICOLAS CABALLERO — Bom dia, boa tarde, boa noite novamente. Bem-vindos a sessão sobre a mitigação do abuso do DNS. Temos a Leticia Castilho, da ICANN Compliance. Siôn Lloyd. Bom, ele vai chegar mais tarde. Graeme do NetBeacon. Levy, de Tucows. Luc e Jeff. Bem-vindos todos.

E os líderes do GAC são Martina Barbero, da Comissão Europeia, e Tomonori Miyamoto do Japão. Vamos falar de detalhes e nuances do abuso do DNS e com isso então eu gostaria de passar a palavra ao distinto colega do Japão, Tomonori Miyamoto.

TOMONORI MIYAMOTO Então, nós somos liderados por Martina Barbero, da Comissão Europeia, que está online. Eu gostaria de saudar a todos aqui da mesa como mencionado. Aqui a agenda para essa sessão. Vamos discutir os resultados da enquete do GAC sobre abuso do DNS.

Teremos uma atualização do Compliance. O relatório INFERMAL e vamos discutir a mitigação. Quais são os próximos passos para mitigação do abuso do DNS. Gostaria de dar o os antecedentes desse tema. A mitigação do abuso do DNS é uma questão importante para o GAC. Já discutimos isso. Aqui em Seattle, na sessão anterior discutimos como SSAC NCSG, os registros de gTLD e os registradores têm a obrigação contratual de responder aos relatórios de abuso do DNS.

Há várias definições do abuso do DNS. Alguns países estão CSAM, e a Associação de Copyright do Japão, e os contratos da ICANN são bem claros. Alguns que se limitam a (inint) [00:04:30] phishing, pharming e spam. Para lidar com esse desafio é importante cobrir os trabalhos realizados dentro da ICANN e compartilhar as boas práticas. Como alguns devem lembrar, esse gráfico mostra o cenário da comunidade da internet.

Nós temos aqui a autoridade contratual, que tem um mandato muito limitado, que é com os registros e registradores. Em vermelho mostramos que muito mais pode ser feito além das obrigações contratuais da ICANN. No outono, discutimos em Istambul sobre o que podemos fazer dentro da ICANN e discutimos com as partes interessadas sobre efeitos das emendas dos contratos e realizamos uma enquete sobre abuso de DNS para que víssemos os resultados e quais eram também as atividades da comunidade em relação ao abuso do DNS.

E nessa discussão, então, vamos discutir os resultados da enquete da ICANN. E também uma atualização do Compliance ou também a apresentação sobre o relatório INFERMAL, métricas de domínio e discussão do GAC sobre as próximas etapas. Uma ideia que temos é que essa cooperação continue ou se estenda a todo o ecossistema.

MARTINA BARBERO

Muito obrigada, Tomo. É um prazer estar aqui e apresentar de forma remota. Eu sou um dos co-líderes do GAC sobre abuso do DNS. Vamos apresentar brevemente os resultados da enquete do GAC sobre abuso do DNS, que foi lançada no início de 2025. Aqui já vemos os resultados. Essa enquete foi planejada de acordo com o objetivo estratégico quatro do GAC. A ideia é fazer uma consulta dos membros do GAC observadores, para saber melhor como abordar as preocupações e atingir as expectativas dos governos.

Então essas questões foram discutidos entre reuniões do GAC e durante as reuniões. Então, recebemos 21 respostas. Vemos aqui a distribuição geográfica. Temos todos os continentes representados com diferentes níveis de participação. E gostaria de agradecer a todos os membros do GAC que responderam à enquete, porque nos ajudou muito saber qual é a sua perspectiva, embora a amostra não seja estatisticamente representativa, pode nos informar para orientar o nosso trabalho, especialmente aos interesses do GAC quanto ao abuso do DNS.

Antes de entrar nos detalhes, eu gostaria de falar dos destaques da enquete. Três principais. Como se esperaria, se confirmou que o abuso do DNS é uma prioridade para os membros do GAC. E a pesquisa também mostrou que os membros do GAC têm diferentes abordagens a esse tópico e diferentes melhores práticas. Então, há uma diversidade em como é abordada essa questão entre os membros do GAC.

O que apareceu também, que é o segundo destaque, é que, em geral, o GAC apoia e agradece o trabalho feito pela ICANN org e a comunidade da ICANN quanto ao abuso do DNS, mas também há um reconhecimento que esse tema é de grande importância e urgência e que precisamos fazer mais. E outro destaque, os membros do GAC acham que o GAC tem um papel importante como parte da comunidade da ICANN no trabalho sobre abuso do DNS.

Há várias coisas que o GAC pode fazer, como monitorar o compliance, através das emendas do contrato, elaboração de políticas, orientações e apoiar a colaboração, como também abordar novas tendências e compartilhar as melhores práticas. Eu queria entrar em detalhes, então, sobre a pesquisa. Uma parte da pesquisa para saber qual é a definição dos membros do GAC do abuso do DNS. As abordagens de melhores práticas para tratar do abuso. A definição de abuso de DNS por membros do GAC.

44 utiliza a definição da ICANN, mas um quarto dos membros tem uma definição mais ampla que inclui dano online, fraude e alguns membros ainda não têm uma definição formal. Como mencionei, os membros do GAC têm diferentes abordagens para o abuso do DNS, que vão desde iniciativas legislativas, marcos de política, cyber iniciativa, colaboração com ccTLDs e outros atores.

Então, uma grande variedade de ferramentas, o que resulta em uma grande variedade de melhores práticas. Entre elas, medidas proativas, parcerias público privadas com partes contratadas como registros e registradores ou outros parceiros da sociedade civil. E temos a adoção de padrões de segurança e o uso de incentivos financeiros, conhecer as iniciativas dos clientes. E o que foi interessante, a inteligência artificial. Já ouvimos falar muito dos perigos da IA, de serem fraudulentas, mas vimos que os membros do GAC usam IA para responder ao abuso DNS.

Em termos de colaboração da comunidade há uma grande variedade de atores que vão desde servidores, provedores de

serviço de internet, forças da lei, e autoridades de IP. 60% dos membros do GAC que responderam, colaboram com outros atores. A segunda parte da enquete, era saber como os membros do GAC monitoram o abuso do DNS.

Então, fontes de dados. Onde acham dados sobre abuso do DNS. Alguns membros do GAC tem sites específicos para que o público denuncie fraude e também podem compartilhar informações com órgãos governamentais e não governamentais e cooperam com CERTs. Alguns membros usam fontes da ICANN como publicações como INFERMAL, que vamos discutir hoje, então diferentes fontes da comunidade da ICANN.

Há diferentes abordagens para coletar dados, mas algumas fontes de dados comuns e queremos saber que tipo de evidências temos que indicam abuso do DNS. Uma parte essencial foi saber como consideram os esforços da comunidade da ICANN para mitigar o abuso do DNS. Quatro perguntas diferentes e cada uma com um grupo diferente, uma sobre avaliação das iniciativas da ICANN org depois dos registros e registrantes em termos se eles efetivamente estavam em conformidade com as obrigações contratuais.

E há uma coerência na classificação e é um pouco menor para a iniciativa das partes contratadas. Mas, em geral, os membros do GAC apreciam as iniciativas da comunidade e as classificam num nível alto. Então, como é que vemos os detalhes aqui? Quanto à mitigação do abuso DNS? Há uma certa satisfação e reconhecimento que o progresso não é tão rápido quanto deveria.

E a eficácia poderia ser maior e então incentivam a ICANN org e o novo CEO que serão mais ambiciosos em seus objetivos.

Quanto às iniciativas das partes contratadas há uma satisfação geral, reconhecendo que existem iniciativas e são significativas, mas também acham que é muita incoerência entre as partes contratadas, algumas ainda fazem o mínimo (inint) [00:17:10], enquanto outros são mais eficazes e dando margem para melhoria.

E quanto à satisfação em relação ao contrato de registros e credenciamento de registradores, foi considerado que é um passo importante, mas não podemos medir ainda sua eficácia. E também as emendas ainda têm lacunas, como por exemplo, não obrigam as partes contratadas a adotar medidas proativas. Relatoria mais transparentes e não cobrem toda a cadeia de valor. Por exemplo, os revendedores não são incluídos. E também houve essa ligação com a exatidão, que não estão nas emendas, mas que o GAC considera importante.

Eu acho que é o meu último slide sobre a enquete. A última parte foi perguntar quais seriam as prioridades em preparação da nova rodada no próximo ano. Conseguimos agrupar as respostas em quatro pilares. Há um papel do GAC para monitorar a implementação das emendas, a conexão com o compliance da ICANN e garantir que as emendas aumentem o nível antes da nossa rodada.

A importância de elaboração de políticas específicas, como por exemplo, tipos específicos do abuso do DNS em adotar medidas

proativas. Há uma lista de tópicos que podem ser relevantes para a elaboração de políticas. Há outro pilar relacionado a produção de orientação e estimular a colaboração. Então, fortalecer a colaboração não é só garantir que o GAC fala com outras partes da comunidade, mas que também ligue isso ao que acontece fora da ICANN.

E alguns membros falaram na necessidade de elaborar orientações de como tratar do abuso do DNS antes da próxima rodada. E finalmente, isso está ligado à nossa discussão com o SSAC, considerar novas ameaças e tendências. A tecnologia nunca para. O progresso tecnológico nunca para. Então, o que podemos aprender quais são os novos, por exemplo, tudo o que tem a ver com inteligência artificial relacionada a ---.

E também compartilhar as melhores práticas entre as comunidades, incluindo os ccTLDs. Por último, as respostas são os vínculos entre o abuso do DNS e o trabalho com dados de registro. Por exemplo, a exatidão dos dados. É uma questão que levamos em conta e acho que esse slide mostra nosso trabalho básico, os principais assuntos a discutir com o GAC. Temos agora uma sessão de perguntas e respostas. Passo a palavra a Nicolas Caballero.

NICOLAS CABALLERO Obrigada. Comissão Europeia, é sempre um prazer ouvi-los e deixamos o espaço aberto para perguntas ou comentários aqui e também online.

MARTINA BARBERO

Há uma pergunta sobre um dos slides que mostrei. O que significam escala, por escala. O que significa um na escala, melhor para pior ou pior para o melhor. A escala que nós utilizamos vai de insatisfeito para satisfeito. É isso.

NICOLAS CABALLERO

Obrigado. Nenhuma mão levantada. Passo a palavra ao representante do Japão.

TOMONORI MIYAMOTO

Eu gostaria de convidar a Leticia.

LETICIA CASTILLO

Sou Leticia Castilho, diretora sênior de Compliance da ICANN. Obrigada pela oportunidade para dar uma atualização sobre a aplicação de requisitos de abuso do DNS. Recebi algumas perguntas antecipadamente que tentei incorporar na apresentação de hoje. Desculpem, não consegui, mas estou aberta para discuti-las depois.

5 de Abril para 5 de dezembro, Compliance resolveu 204 investigações que levaram a uma suspensão de mais de 2.900 nomes de domínios maliciosos e desativaram sites por phishing, 365. Então, como falei, a suspensão em 2.900 nomes de domínios maliciosos e desativação de 365 sites por phishing. E desde 5 de março de 2025, semana passada, tivemos 45 investigações em

andamento sobre mitigação de abuso com mais de 5.400 nomes de domínio maliciosos já mitigados, mais de 89% dos casos envolvendo phishing.

E isso, além dos planos de remediação que as partes contratadas simplesmente como é implementado para os casos de compliance, além das ações que os registradores e registros adotam para combater o abuso do DNS para cumprir com o contrato e enviamos três notificações formais de quebra relacionado com os novos requisitos e abusos do DNS. É uma notificação de violação emitida quando o estado informal do progresso ficar exaurido, sem resolução e tipicamente compreende três notificações: chamadas telefônicas, contato com as partes e oferecer informações.

O processo então foi expedido, como por exemplo, quando descobrimos falhas repetidas de violações que foram remediadas anteriormente. Três notificações de violação que estão em andamento e enquanto continuamos a monitorar e remediar a situação e quanto a extensão de prazos, isso não é muito comum quando as partes contratadas estão implementando planos de remediação, mas sob certas condições, sim.

Por exemplo, quando não é outorgada uma extensão em nomes de domínios abusivos identificados, isso continua a estar ativo, prolongando a exposição a potenciais vítimas. Temos 46 investigações agora em andamento. Já falei isso. Aproximadamente 48% delas resultaram da ação de denúncias encaminhadas por pesquisadores em segurança, também por

advogados e associações. Aproximadamente 15% das quais 13% de nossas reclamações escolheram a categoria dentro do formulário e costumam ser representadas por companhias e 24% esteve composto por outras porcentagens menores, outras partes contratadas, registradores, etc.

Quanto à distribuição geográfica, os reclamantes comentaram que denunciaram na região Ásia-Pacífica, América do Norte mais do que na Europa e na América Latina, como nós vemos aqui e além da aplicação de todos os requisitos de mitigação de abusos, nós fazemos duas rodadas de auditorias por ano. Temos uma equipe dedicada ao sistema de compliance, temos a KPMG, que existe na coleta e avaliação de dados.

As auditorias podem informar casos de violação. Isso no final de cada rodada. E em outubro 2024, lançamos uma auditoria que incluiu requisitos de abuso do DNS e as perguntas na auditoria buscavam verificar se os registros entendiam as alegações e aplicavam processos para mitigar isso. Isso esteve baseado em pontuações internas e externas, mas não significa que haja um não cumprimento e todas as partes auditadas encaminhar as informações e documentos exigidos e revisamos as respostas e esclarecimento e solicitamos mais informações.

Aqui resumimos algumas das iniciativas em que estamos trabalhando. Planejamos emitir um relatório a cada ano e incorporando o feedback recebido em volume e que vai incluir mais informação sobre o processamento de reclamações e

também questões de material educativo. E também mais detalhes sobre ações de aplicação da lei com uma atitude proativa e novas iniciativas, materiais de educação. Tudo isso, além das auditorias, e estamos comprometidos com continuar informando sobre os nossos progressos.

NICOLAS CABALLERO: Obrigado, Leticia. Fantástica apresentação, com muitos detalhes. Vamos fazer uma pausa. Vamos ver se há perguntas ou comentários aqui na sala ou online. Não veja nenhuma mão levantada online. Nem na sala, mas sim, temos a Índia. Representante da Índia. Pedimos que tente falar divagar. Eu sei que em benefício da interpretação, é necessário falar lentamente.

NÃO IDENTIFICADO: Obrigado, senhor presidente. No relatório destacaram que às vezes há diferentes grupos de criminosos que têm a ver com os registradores. Não sei se isso tem a ver com o modelo de preços, porque há alguns processos que às vezes têm a ver com algum tipo de qualificação de risco dos registradores e isso com base nos achados na auditoria, ou se estamos iniciando mecanismos para registradores.

LETICIA CASTILLO: Vou tentar repetir a pergunta, vou ver se entendi bem, tem a ver com o gráfico que eu mostrei ou é algo geral?

NÃO IDENTIFICADO Não, em geral, não especificamente da apresentação. Mas a pergunta é: essas auditorias emitem relatórios formais e alguns registradores têm uma qualificação baixa quanto aos processos, ou medidas de mitigação de abuso.

LETICIA CASTILLO Essa auditoria ainda está em andamento.

NÃO IDENTIFICADO Mas temos repetição de abusos dos criminosos e eu não sei se isso tem a ver com o relatório formal, mas a ideia é e é uma boa ideia, não sei se ter algo que começa com uma métrica de avaliação talvez, para fazer uma qualificação de registradores.

LETICIA CASTILLO Não sei se entendi bem a pergunta, mas sob a perspectiva de compliance nós devemos executar os contratos, fazer com que sejam cumpridos, então nós, em compliance, coletamos muitos dados, os revisamos e anteriormente eu mencionei que parte dessas iniciativas em que estamos trabalhando para fazer um monitoramento proativo, a iniciativa de execução proativa, os dados coletados que têm a ver com falhas repetitivas e com alguns padrões repetitivos e alguns registradores que mostram mais falhas do que outros. E tudo isso é levado em conta na planificação dessas ações de aplicação proativa. E nós aplicamos isso,

executamos, mas sempre podemos levar em conta alguns padrões de forma específica. Não sei se estou respondendo a sua pergunta.

NICOLAS CABALLERO Agora é a vez do Gabriel Andrews.

GABRIEL ANDREWS Obrigado pela apresentação. Uma dúvida, quando vocês falam sobre a grande quantidade de dados que recebem, que vocês estão investigando. São 46 esse ano e são muitas. Mas eu me pergunto que tipo de dados são esses? Que dados vocês pedem dos registradores? E esses dados não incluem informação de registros, registrante, os titulares de conta, todos que participam desses 5.400 domínios maliciosos?

LETICIA CASTILLO Quando iniciamos uma investigação em compliance, a ideia é ver as obrigações específicas incluídas na denúncia ou reclamação e podem ter a ver com dados vinculados a alguma inexatidão, com alguma obrigação contratual. E como isso depende dessa reclamação, em geral, oferecemos uma cópia da reclamação, uma segunda via da nossa prova e mencionamos qual é o ponto importante que nós devemos abordar para o registrador e pedimos uma descrição detalhada da parte contratada de como foi enfrentada essa ação para reduzir, mitigar e deter ou interromper essa ação.

E às vezes, quando estamos explicando a investigação, o registrador menciona todos os casos. Às vezes podem realizar verificações de todas as contas, mas nós, o que nós pedimos, é especificamente aquilo que é necessário para investigar.

NICOLAS CABALLERO Fala República Dominicana.

NÃO IDENTIFICADO Vou falar espanhol. Leticia, obrigada. Comentário breve agora e depois uma pergunta. E eu saio daqui mais tranquila, porque na sessão anterior que foram mencionados os abusos DNS, eu não fiquei tranquila. Mas agora eu vejo que sim, que há um acompanhamento, está sendo muito trabalho, porque o que mencionou a Leticia está sendo feita muita coisa, o que me deixa tranquila como representante do meu governo.

Então pergunta: essas auditorias, esses relatórios estão publicados online e podem ser consultados? Porque para nós, nas nossas estratégias em cibersegurança, em que nós também seguimos abuso infantil, violência da mulher, etc. A auditoria poderia ser um material muito construtivo para nós, para aprender mais sobre como lidar com isso e o que está acontecendo, quais são as tendências. Obrigada.

LETICIA CASTILLO Vou responder em espanhol. Obrigada pelo comentário e pela pergunta. Sim, nós capturamos muita informação e dados

recebidos e processados e também temos relatórios que são publicados mensalmente, que incluem não apenas as obrigações de usos do DNS, mas outras obrigações de acordos da ICANN. Mas nós temos um relatório, um contrato dedicado sobre requisitos que é publicados esse relatório mensalmente, com muitos dados, está dividido de acordo ao tipo de abuso do DNS.

Também publicamos um relatório com mais dados e exemplos e contexto, porque às vezes muitos dados, só apenas dados não basta. Precisamos de exemplos. E esse relatório foi publicado em 8 de novembro no nosso site. E também estamos trabalhando em publicar um outro relatório com mais contexto, mais exemplos e incorporamos um feedback da comunidade. E esse relatório anterior vai ser publicado depois de um ano dos requisitos e as auditorias também, têm seus próprios relatórios que são publicados.

NICOLAS CABALLERO Bom, agora vem a Suíça e depois eu vou ter que encerrar a fila. Devemos continuar com as apresentações. Pode falar porque, Jorge Cancio.

JORGE CANCIO Obrigado, Nico. Obrigado pela sessão, especialmente a Leticia Castilho pela informação. Eu gostaria de dar algumas opiniões sobre conversas com a Polícia Federal na Suíça. Eles vêem que há um efeito positivo das emendas nos contratos. É um bom sinal. E

eles vêm que alguns registradores não estão colaborando tanto quanto precisariam. Portanto, temos dúvida sobre o que que pode ser feito para aumentar os incentivos para esses registradores que não estão colaborando, que parece que não estão seguindo o que nós recomendamos.

Portanto, se houver alguma maneira direta de notificar o departamento de Compliance, seria muito bom ter esses dados, porque seria algo muito importante para nós. O que recebemos como feedback, que atualmente nos órgãos de aplicação da lei quanto a denúncias de abusos, nem sempre são levadas a sério. E há preocupações a respeito disso, porque a legitimidade é discutida às vezes. E embora as fontes sejam legítimas.

LETICIA CASTILLO

Quero ver se eu me lembro de tudo o que eu queria dizer. Nós incentivamos que essas denúncias sejam feitas a nós. Temos formulários online, são públicos. Algumas perguntas dos formulários com o objetivo de coletar informações. Se a denúncia foi feita pelas forças da lei está sendo monitorado no nosso sistema.

Nós incentivamos a todos que denunciem a nós se acham que está havendo uma violação contratual. Como nós falamos, que se não há resposta ou se a violação resultar em uma (inint) [00:43:38] formal, o registro é suspenso ou cancelado. Nós prestamos atenção as denúncias de todos. Não sei se estou certa, mas quando se faz uma denúncia dizer que a força da lei de tal órgão e qual é a

sua jurisdição. Quando isso não fica claro, pedimos mais informações, isso não quer dizer que não vamos levar isso adiante. Mas dependendo da jurisdição, nós precisamos saber a qual a parte deve ser contratada.

NICOLAS CABALLERO Precisamos continuar com a apresentação. Passo a Tomo.

TOMONORI MIYAMOTO Muito obrigado pela atualização. E eu espero ansiosamente pelos próximos relatórios. Eu convido da OCTO, Siôn Lloyd para a apresentação do relatório INFERMAL e as métricas domínio.

SIÔN LLOYD Eu sou Siôn Lloyd e eu trabalho para a diretoria de tecnologia da ICANN. Eu vou falar de duas partes diferentes: a métrica dos domínios e o relatório INFERMAL. Em primeiro lugar, métrica de domínios. O que é o sistema de coletar dados de nomes de domínios e tornar esses dados buscáveis, utilizáveis, possíveis de fazer o download em diferentes formatos para o máximo de usuários possíveis.

Nós temos os dados de nomes de domínio e podemos agregá-los em nível de gTLD e registrável, vocês podem obter metadados relativos ao domínio ou registrador ou TLD que você está procurando. Nós temos dados em níveis também que podem ser

compartilhados. Vocês podem usar uma interface. E interfaces com pela internet e um API.

Então eu não posso mostrar todas as funcionalidades, mas eu quero mostrar alguns exemplos excelentes. Se você receber um texto ou e-mail com um nome que você não conhece, você pode consultar as informações de antecedentes, qual é o registrador, quando foi criado, algumas configurações do DNS e também vocês verão se vocês podem ver se nós sabemos de alguma denúncia de abuso.

Além disso, uma linha de tendência que mostra a popularidade do domínio, o que dá uma ideia se esse nome tem uma boa reputação. Se pode fazer a mesma pesquisa em nível de TLD. Temos a informações, o registro, qual foi a mudança, o tamanho de zona e estatística sobre a quantidade de abuso denunciados. Contagens do domínio e a percentagem do tamanho do domínio.

Também se obtém outras informações, com tendência dos abusos denunciados e onde estão esses domínios. Então se vê onde estão hospedados. Falamos dados em nível de domínio compartilháveis para registros e registradores que usam o sistema. Então, você tem uma lista de nomes que estão sob o seu registro e vão dizer quem denunciou o domínio, que tipo de abuso.

Então, se vê denúncias de botnet, malware, mas a grande maioria é phishing. O domain métrica não é um produto acabado. Nós achamos que vai evoluir ao longo da vida, agregando novas métricas, fontes de dados. É uma plataforma onde podemos

publicar os dados, os resultados das nossas pesquisas e também o feedback da comunidade.

Qualquer um que tem uma conta na ICANN, quando você se inscreve no ICANN, você tem acesso ao domain métrica. Alguns links aqui. É uma página que dá mais detalhes, as perguntas frequentes, a documentação e outro link é de um webinar que dá mais detalhes das funcionalidades dentro dessa plataforma domain métrica.

Então, eu vou falar agora do relatório INFERMAL, que foi publicado no ano passado. Esse é um projeto financiado pela ICANN. O trabalho foi realizado por um grupo sob o professor Maciej Korczyński, do KOR Labs, da Universidade de Grenoble. E avaliou as políticas de registro para revelar padrões de preferências de atacantes de TLDs. Então, o relatório final foi publicado no final do ano passado e mais detalhes vocês podem encontrar nessa página.

Esse relatório é muito detalhado e abrangente. E houve um webinar que foi feito no início desse ano sobre esse tema. O que o INFERMAL fez, olhou diferentes características de um registro: preço, descontos, podem ser descontos, se você registra um grande número de domínios, você tem uma tarifa menor por registro; instalações para registros em massa, a presença de uma dessas interfaces. Então quanta automação é possível durante o processo de registro.

Por exemplo, se pode pagar com PayPal, se pode pagar com criptomoeda, quais são os serviços gratuitos: hospedagem,

certificado. Quanto disso é oferecido como parte do processo de registro. Outro grupo de funcionalidades como verificação ou práticas de verificação e segurança. Por exemplo, validação dos detalhes de contato antes do pagamento ser aceito para o registro.

Quais são os registros, é necessário presença na jurisdição do país onde você está fazendo o registro. Documentação, que medidas proativas estão sendo tomadas para evitar o registro de nomes potencialmente abusivos. Por exemplo, se alguém tentar registrar Office 365 ou Facebook, esse tipo é uma um alvo de phishing. Além das medidas proativas, as reativas.

Então, em quanto tempo os domínios permanecem ativos antes do abuso ser mitigado. Diferentes conjuntos de dados foram utilizados. Eu não vou falar de todos. É uma mistura de dados de terceiros, dados coletados manualmente e com medidas ativas, como medidas do DNS e WHOIS. Então, o relatório em si é muito detalhado e dá o contexto de todos esses dados.

Eu não posso fazer isso nesses poucos slides. Então, isso é o que nós estamos vendo. Quais as correlações mais fortes com o aumento do abuso, a disponibilidade gratuita de APIs, serviços extras fornecidos, DNS gratuito, hospedagem e descontos no registro. E, por outro lado, as correlações mais fortes com a redução do abuso foram medidas proativas, como validação dos dados de contato antes do registro.

É possível que, com esses fatores, isso seja atraente para ataques resultando de uma diminuição de fatores e decisões tomadas

sobre esses dados. Por exemplo, uma decisão talvez signifique que os criminosos, hackers, tenham uma menor preferência por um TLD em particular ou em um registrador, mas também vai afetar usuários legítimos. Qualquer medida, então, vai afetar os usuários legítimos e também os hackers. E eu gostaria de agradecer o professor Korczyński e sua equipe pelo trabalho profundo que fizeram. Então, fico aberto para perguntas.

NICOLAS CABALLERO Muito interessante a sua apresentação, especialmente coisas muito simples como o número de telefone e o e-mail, essas exigências fazem com que o abuso diminua. Temos os dez minutos. Então, o microfone está aberto. Eu vejo que aqui alguém levantou a mão. Pode usar qualquer um dos microfones.

ALEX URBELIS Eu sou Alex Urbelis. Eu tenho uma pergunta do métrica e estatísticas que vocês coletam. Você mencionou que você está rastreando a localização do host. Muitos dos atacantes se ocultam numa nuvem. Então, como é que vocês coletam as informações?

SIÔN LLOYD Só geolocalização do endereço de IP. Nós sabemos que pode haver aí incoerências e imprecisões, mas esses dados são atualizados em tempo real, diariamente. Então, eu posso denunciar um domínio e esses dados serão atualizados imediatamente.

TRACY HACKSHAW Quanto a métrica, eu estava olhando o site. Eu queria saber se é possível fazer comparações? É possível comparar um TLD com o outro?

SIÔN LLOYD Sim, podemos fazer isso se interagirmos no chat. Então, depois dessa sessão aqui, a gente pode falar, eu posso te mostrar como isso é feito.

NICOLAS CABALLERO Muito obrigado, UPU. Alguma pergunta ou comentário antes de continuarmos? Desculpe. Camboja pediu a palavra.

NÃO IDENTIFICADO Bom dia a todos. Eu sou da Camboja. A minha pergunta talvez seja para o presidente do GAC. Há alguma regulamentação ou orientação ou relatório detalhado sobre o abuso do DNS ou decisão regulatória para a auditoria do abuso do DNS. Hoje de manhã ouvimos falar de compliance e mitigação. Mas há alguma regulamentação para proteger contra o abuso do DNS?

NICOLAS CABALLERO Eu não entendi bem a sua pergunta. Exatamente o que você está perguntando?

NÃO IDENTIFICADO O GAC ou ICANN tem alguma regulamentação, uma orientação para a proteção contra o abuso do DNS ou não?

NICOLAS CABALLERO A resposta curta: há várias recomendações da ICANN e do Instituto NetBeacon e outras instituições. Podemos indicar como a implementação do DNSSEC, temos uma equipe fantástica dentro da ICANN que podem ajudar. Não só com a implementação do DNSSEC. Então, por exemplo, o MANRS, que são normas mutuamente acordadas para a segurança de roteamento que podem ser implementadas no seu país. Mas não existe um pacote pronto. Muito obrigado pela pergunta. Precisamos seguir adiante.

TOMONORI MIYAMOTO Vamos passar para a discussão do painel. Nós temos NetBeacon, Reg vai, das partes contratadas. Essa pergunta são os tópicos da discussão hoje. E quais são as tendências. Então, nós teremos o Graeme Bunton sobre esses temas.

GRAEME BUNTON Muito obrigado. Sou Graeme Bunton, diretor executivo de NetBeacon. Trabalhamos por uma internet mais segura para todos, reduzindo a prevalência de nomes de domínio malicioso. Parabéns para o professor Korczynski, da ICANN e a equipe da OCTO pelo trabalho feito com o relatório INFERMAL, que é interessante, importante e útil.

Esse era o trabalho que a gente queria fazer, vocês o fizeram antes, mas esse relatório, o trabalho, esse relatório destaca a complexidade de diminuir o abuso e devemos (inint) [01:04:24] uma das características identificadas como um botão de ajuste, que é um botão que cada registrador deve ajustar. Devemos pensar em cada um desses problemas e o INFERMAL deu dados concretos sobre problemas, que nós consideramos que estão envolvidos no abuso do DNS como comunidade e também, por exemplo, preços ou APIs.

E realmente a baixa relação entre a velocidade de mitigação e abuso é algo que me surpreendeu. Eu pensava que isso era uma ação muito rápida, ação de mitigação, o que seria menos atraente para os criminosos e é importante considerar isso nessa comunidade. E o que deveríamos fazer então, como comunidade, há interesse em ter um PDP sobre abusos e antes disso, deveríamos estabelecer alguns princípios, como prestar atenção a sondagens e estudos, por exemplo, acelerar o processo e primeiramente seria identificar.

Um problema específico o qual poderia produzir um progresso incremental. Devemos então identificar problemas específicos e avançar de forma muito específica, super específica. Tão específica que a pessoa se sinta incômoda, porque é tão limitado que devemos fazer com o que temos, então progressos em muito pouco tempo. E depois, bom, se tivermos um PDP não deveria levar em conta a tecnologia e os modelos de negócios.

Pensemos como seria esse trabalho. Então, lembremos que os criminosos são mais rápidos, mais inteligentes, não têm limitações e às vezes têm melhores recursos que a gente. E eles não seguem as nossas regras e não podem produzir políticas que especifiquem limites sobre serviços. Por exemplo, podem atuar em questão de horas, enquanto para nós, fazer uma política leva anos. Eles já têm que encriptação, tem automação, já tem tudo. E o que é que nós podemos fazer?

Devemos identificar mudanças de políticas potenciais para fazer esses ajustes necessários para implementar atritos contra os criminosos, que tenham impacto nos criminosos e que sejam aplicáveis e auditáveis. Então, vou tentar ser mais concreto. Falamos antes do acesso a API gratuito também. Então, como fazemos com que os registrados sejam mais cautelosos sobre como acessar algumas funcionalidades? Para isso, poderíamos ter políticas efetivas para lidar com isso, que estejam adaptadas ao mercado.

Depois, quanto aos dados e relatórios ou denúncias de abusos. Temos isso a cada dia. Temos uma métrica, uma funcionalidade, que é uma métrica disso e o fazemos a cada dia e começamos a ver as taxas de mitigação, depois de ter feito as emendas. E é importante então verificar isso e ajuda muito. E é isso que eu queria mencionar.

TOMONORI MIYAMOTO Obrigado pelos comentários.

REG LEVY Queria destacar algo que indicou na apresentação um site pelo qual o pessoal pode enviar denúncias. É um espaço centralizado no site para fazer denúncias e que tem na NetBeacon no seu portal. E seria necessário ter isso também em nível da União Europeia.

JEFF BEDSER Obrigado. Já falamos no contexto de SSAC esta semana e eu queria destacar também que o relatório INFERMAL foi excelente. Parabéns para os pesquisadores e a OCTO. Mas não é um relatório de recomendações, é apenas de achados e confirmou coisas que já sabíamos ou suspeitávamos aliás, já faz um tempo. Mas as pessoas sempre compram o recurso mais barato e mais fácil de encontrar.

Quando observamos os cyberdelitos, vemos o que facilitou, principalmente pelos domínios. Tem um braço que vai de um a 10 trilhões e são incentivos para criminosos que é para utilizar domínios para roubar os cidadãos de todos os países. E, às vezes, não é uma questão de quantidade de dinheiro. Para mim, há soluções reais para o futuro. Não é o que fazemos para evitar que certos domínios sejam vendidos para alguns usos determinados, usos abusivos.

O que a maioria das denúncias são utilizadas para medir o problema, cinco a sete deles são apenas a ponta do iceberg. E cada registro ou registrador recebe milhares de denúncias por ano e não

pode fazer muito para lidar com todos eles. E acho que todos aqui, tenho certeza na sala, deve ter tido algum tipo de caso ou tem casos de phishing várias vezes ao dia e sabemos que isso é muito grande e a melhor maneira de lutar contra isso e funcionar, ter um melhor modelo para funcionar como comunidade da forma mais rápida possível, para poder rapidamente medir os eventos.

É isso que deve estar inserido nas obrigações contratuais e que os ccTLDs devem fazer um relatório de provas e que funcionem mais rapidamente. Não é uma questão de reinventar ou reinvestigar uma denúncia, mas sim, devemos ir nessa direção e espero que esse relatório INFERMAL tenha excelentes resultados e que sejam claros para a economia, com soluções baseadas em melhores denúncias e melhor detecção dos abusos. Obrigado.

TOMONORI MIYAMOTO Obrigado, Jeff. Então o espaço fica aberto para discussão, comentários ou perguntas. Aqui alguém.

REG LEVY Eu gostaria de destacar também o excelente trabalho que o Jeff e sua equipe estão fazendo na NetBeacon com tecnologia que são excelentes e trabalham certamente com CleanDNS. E isso também com a União Europeia e o que observamos que é muito utilizado para criar mais abusos do DNS. Parece cômico, mas não. A tecnologia do Jeff tem muitas ferramentas que poderiam ajudar a obter mais informações para agir melhor e mais rapidamente.

NICOLAS CABALLERO Aqui temos uma pergunta do público.

DEAN MARKS Muito obrigado. Sou Dean Marks, do grupo de Propriedade Intelectual. Uma pergunta para Jeff. Você destacou o importância das denúncias e a detecção e o trabalho que você fez parece ser mais reativo, mas você tem algumas reações sobre passos ou pensamentos, sugestões sobre passos que poderiam ser dados no sentido preventivo de abusos do DNS? Você mencionou os preços que não importam tanto a um preço mínimo entre 1.000, mas isso não importa tanto para o cyberdelito. Então qual seriam medidas preventivas? Por exemplo, conhecer o cliente? O que você acha?

JEFF BEDSER Obrigado. Excelente pergunta. Sim. Conhecer os processos do cliente, a validação também são importantes. Eu já falei sobre isso. O potencial da IA para criar novas identidades, IA generativa, por exemplo, criando identidades. E vemos esse crescimento. E vemos que em alguns casos, já há soluções e eles têm uma solução para o problema, eles querem que o domínio tenha uma extensão similar, passam por esse processo para obter o domínio. Isso já está demonstrado. Eu já vi esforços entre registradores e registros e amanhã vamos falar mais sobre isso.

Mas essa colaboração, cada um deles processa milhares de denúncias por ano e a infraestrutura que está por baixo dessas

denúncias poderiam ter um padrão para detectar mais ou, por exemplo, o criminoso que opera registros e registra um domínio que a Tucows observa e a bloqueia, esse já é um padrão, uma repetição.

Os domínios são perecíveis e, às vezes, é mais difícil de manter um desses nomes de domínio, é melhor então bloqueá-lo, porque tem um problema de reputação, é difícil de resolver e temos processadores pelos quais vários sites passam por phishing ou utilizem cartões de créditos e é possível atacá-los nos seus sistemas de processamento de pagamento.

NICOLAS CABALLERO Obrigado, Jeff. Antes de passar para o Reino Unido. Graeme tem alguma coisa para mencionar?

GRAEME BUNTON Sim. Vou tentar ser breve. O Jeff já falou muito, mas uma das partes dentro do relatório INFERMAL e que destaquem e que aumentam o KYC e acho que podemos melhorar na identificação de identidades e pode ser uma parte da solução, não é a única solução, mas é uma parte. E também há outras oportunidades que são interessantes de serem exploradas fora do contexto da ICANN, como a relação entre fraude e abuso e ver que tecnologias e ferramentas podemos utilizar aqui. E esta semana houve alguém que mencionou que estavam falando que todos os seus abusos foram comprados com cartões de crédito legítimo. Isso foi para mim uma grande surpresa.

NIGEL HICKSON

Eu me perguntava que assunto tão complexo sim. E os adversários que estão aumentando e ver como nós nos conduzimos nesse sentido contra os criminosos. E o caráter INFERMAL, eu acho que é muito interessante. Tivemos discussões faz uns anos, não tínhamos tantas provas, mas agora sim, temos provas. Eu acho que provavelmente, hoje a tarde a recomendação não mencionemos isso sobre domínios expressos, domínios, mas questões de concorrência, não.

Mas pelo que eu acho, poderíamos incluir algo nos PDP sobre os registros em algumas áreas. Especificamente quando tivermos registros inteiramente gratuitos de domínios. E talvez isso deixe um espaço para mais perguntas que possam ser formuladas. Você está fazendo isso, porque é um evento (inint) [01:22:09] ou perguntas X. Mas acho que deveríamos fazer ainda mais para averiguar o porquê de certos nomes de domínio. Obrigado.

REG LEVY

Estamos observando os registros em massa e também com esta equipe que elaborou e publicou o INFERMAL, onde encontramos, por exemplo, 50 nomes de domínio ao mesmo tempo e não sei se podemos proibi-los ao mesmo tempo ou um deles. Mas com o INFERMAL o que vamos fazer depois é se os dados são dados ruins de uma certa maneira, isso nos vai dar algumas hipóteses, uma série de nomes de domínios e registradores envolvidos no

	INFERMAL, ver se há correlação ou não entre eles. Sim, absolutamente estamos observando isso agora.
NICOLAS CABALLERO	Obrigado, Reg. Fica o espaço aberto.
JEFF BEDSER	Eu fiz a análise. Quando a gente fala de registros em massa, considere como um modelo de licenciamento. Se você tem uma scooter, alguém tenta quase na idade de ter uma carta. Então, uma lambreta você pode obter uma habilitação, mas não para dirigir um caminhão. Então, um registrador que tem um modelo de registro em massa, eles têm requisitos e padrões muito mais altos, porque senão você perde dinheiro, porque essa ferramenta, se ela for mal utilizada, ela pode causar muito dano. Muito obrigado.
TOMONORI MIYAMOTO	Nós teríamos então a o debate aqui, mas parece que o debate já começou.
MARTINA BARBERO	Nós esperamos ser uma excelente sessão. E eu esperava isso mesmo. Seria importante saber o que o GAC acha e ter a contribuição do GAC. E como isso afetaria o abuso de DNS. Nós temos cinco minutos, talvez, quais seriam os próximos passos. Se pudermos discutir também, se vocês quiserem considerações para o comumniqué relacionada a expectativas de futuras atividades,

	considerações para a próxima rodada de novos gTLDs, também discussão com a nossa comunidade, que é o ALAC está interessado em colaborar mais conosco sobre esse tema.
NICOLAS CABALLERO	Nós temos três minutos para rápidas perguntas ou comentários online ou na sala.
DAVID HUGHES	David Hughes, IPC. Eu queria perguntar para o Jeff e Graeme uma pergunta. Vemos que alguns ccTLDs que têm níveis muito baixos de abuso do DNS. O que a gente pode aprender desses ccTLDs?
JEFF BEDSER	A maior preocupação em responder, embora os gTLDs tenha uma série de regras em comum. Os ccTLDs não. Às vezes há uma baixa taxa de abuso. Às vezes está relacionada a uma baixa taxa de crescimento, mas há dois tipos de abuso no nível meta que o domínio é registrado para abuso. Então usamos. Nossos estudos, tudo o que fizemos para gTLDs usamos os meus modelos para ccTLDs. Temos ccTLDs que têm uma das taxas mais altas de abuso. As taxas e vários gTLDs tem baixas taxas também de abuso.
GRAEME BUNTON	É difícil responder. Eu tenho 73 funcionalidades que foram ou características que foram avaliadas. É difícil encontrar uma solução, uma única solução. Eu acho que não se deve ser olhar só

as taxas de abuso. Porque muitas vezes eles utilizam um TLD que o registro não tem um controle maior e eles sabem disso. Precisamos de uma visão mais sofisticada da cadeia do abuso.

REG LEVY

Do grupo dos ccTLDs ou do grupo dos registradores e amanhã vamos falar com ccTLDs. Mas não só os ccTLDs tem diferentes políticas, mas mercados diferentes. Alguns tipos de abuso que podem ter como alvo alguns ccTLDs. Há diferentes fatores que estão envolvidos. Então convido vocês a participar da nossa seção com ccTLDs.

FINN PETERSEN

Finn Petersen, da Dinamarca. Eu acho excelente olhar. Certos ccTLDs, eu sei que algum país o registro em massa foi limitado a cinco. E também há uma investigação detalhada sobre a identidade de quem solicitou. E seria interessante talvez propor um PDP muito específico sobre registro em massa.

NICOLAS CABALLERO

Se bem específico, talvez possa ser adotado e o trabalho começar imediatamente, porque isso já é uma fruta esperando para se colher. Qualquer coisa em menos de cinco anos seria excelente. Bom, agradeço a todos aqui da mesa de consultas. E agradeço muito. Vamos ter agora o intervalo para o almoço. Voltamos à 1:15. Agradeço a todos. Essa sessão está encerrada.

[FIM DA TRANSCRIÇÃO]