
ICANN73 | Fórum virtual da comunidade – Sessão do GAC sobre abusos do DNS e atualização do PSWG
Terça-feira, 8 de março de 2022 – 14h30 às 15h15 AST

GULTAN TEPE: Bem-vindos, aos grupos de trabalho de segurança e investigação de abuso do DNS, na terça-feira 08 de março de 2022, não teremos tempo de fazer a chamada, a participação do GAC será registrada nas atas para garantir a transparência do modelo multisetorial da ICANN, pedimos que vocês mudem seu nome, coloquem seu nome completo e sua filiação, tiverem alguma pergunta ou comentário utilizem os colchetes para indicar questiona ou comment, a interpretação inclui os seis idiomas da ONU e português, podem selecionar o idioma que quiserem ouvir utilizando a funcionalidade de interpretação na barra de ferramenta do zoom, como todas as outras reuniões, essa reunião é governada pelos padrões esperados de comportamento da ICANN, com isso passo a palavra à presidente do GAC Manal Ismail.

MANAL ISMAIL: Muito obrigado por voltarem, espero que tenham aproveitado o intervalo, nós teremos 45 minutos sobre mitigação do abuso do DNS, e 45 minutos procedimentos subsequentes de rodadas de novos gTLD's, os oradores convidados, vão falar pelo grupo de trabalho de segurança pública Laureen Kapin, da comissão federal de comércio dos Estados Unidos, o Chris Lewis Evans da agência de departamento de segurança do Reino Unido, Gabriel Andrews do FBI, pelo GAC vai falar Sumitaka

Observação: O conteúdo deste documento é produto resultante da transcrição de um arquivo de áudio para um arquivo de texto. Ainda levando em conta que a transcrição é fiel ao áudio na sua maior proporção, em alguns casos pode estar incompleta ou inexata por falta de fidelidade do áudio, bem como pode ter sido corrigida gramaticalmente para melhorar a qualidade e compreensão do texto. Esta transcrição é proporcionada como material adicional ao arquivo de áudio, mas não deve ser considerada como registro oficial.

Shirakabe, do Japão, do Ministério do Interior e Comunicações, e a oradora convidada Ivet Paulovics, coautora do estudo da Comissão Europeia sobre abuso do DNS, temos muito a falar então sem mais delongas, eu passo a palavra aos oradores.

LAUREEN KAPIN:

Vou falar dessa vez como copresidente do grupo de trabalho de segurança pública do GAC, então essa é uma agenda dessa sessão então porque que a mitigação do abuso do DNS é importante, teremos o estudo da Comissão Europeia sobre abuso do DNS, e os autores vão apresentar informações desses estudos, e vamos falar de outras atividades recentes como a nova iniciativa que é a iniciativa de facilitação de segurança do DNS, um grupo de trabalho sobre isso, o SSAC 115, a nova ferramenta de relatoria de denúncias de abuso centralizada, cart, e o pequeno grupo da GNSO sobre abuso DNS, e vamos falar um pouco sobre a sessão plenária, sobre abuso DNS que será na quarta-feira, falando a diferença de domínios registrados de forma maliciosa e comprometidos, e depois vamos ouvir o nosso colega do Japão que vai mencionar cláusulas de contrato aperfeiçoadas e as melhores práticas.

Então novamente queremos sempre falar dos antecedentes, das questões discutidas vamos ouvir muitas definições aqui, mas queríamos falar dos antecedentes sobre amplitude das definições, o abuso do DNS é entendido como uma ameaça à segurança, como phishing , malware, botnet, e isso foi retirado da recomendação de salvaguardas do GAC em Pequim, o que é isso, como está estabelecido

no contrato, mas há outras definições também como concorrência, a opção do consumidor, confiança do consumidor a uma definição que foi parte do estudo anterior da ICANN, ou no documento anterior da ICANN, que fala de antiguidades intencionalmente enganosas ou não solicitadas que ativamente utilizam o DNS, e essa definição, é citada na declaração do GAC sobre abuso do DNS, de 2019, e ameaça os consumidores, usuários, individuais ou empresas, e sua confiança na internet, ou uma ameaça à segurança, estabilidade, resiliência na infraestrutura do DNS, isso é parte dos estatutos da ICANN, então quando falamos DNS queremos dizer sistemas de nomes de domínio.

O grupo de segurança pública do GAC, foi formado por causa do... Para estudar os aspectos dessa política e procedimentos da ICANN, que tem a ver com segurança do público tem a ver com atenção dos consumidores, e também fazer recomendações, e dar apoio ao GAC, sobre esse tema. E o nosso grupo foi formado em 2015, temos um plano de trabalho, e levando em conta todos os aspectos formais desse grupo, mas não é só o GAC, e o grupo de trabalho e segurança pública do GAC, mas vários outros grupos da ICANN, e estão tratando da questão do abuso do DNS, levando em conta que os contratos atuais da ICANN não têm obrigações claras, e vinculantes, para mitigar o abuso do DNS, e as discussões da comunidade sobre o compliance dos contratos, a correspondência, com a parte constitutiva, empresarial em 2020, 2019.

E também o GAC fez contribuições em diferentes momentos inclusive em equipes de revisão, e comentários públicos, e participação nas iniciativas de elaboração de políticas. Nesse slide, tem links muito interessantes e uteis que vocês podem utilizar para ler depois. Vamos

falar sobre as iniciativas recentes, em primeiro lugar, há um estudo bastante detalhado sobre abuso do DNS pela comissão Europeia, e com isso então quero passar para a minha colega, esse foi um novo estudo encomendado pela Comissão Europeia encomendado dia 31 de janeiro, e foi comunicado, nós fizemos observações gerais, esse estudo é muito prático, ele enfoca não só os papéis e as responsabilidades, não só nas vítimas e nos criminosos, e não só as partes contratadas da ICANN, mas não partes, mas entidades, mas também, outros que são parte desse sistema, nós estamos só falando sobre o que os registros e registradores podem fazer, mas também sobre outros intermediários, como distribuidores.

E eu acho que as informações dos consumidores tem que ser incluída aí. Muitas das recomendações e observações feitas pelo estudo, também foram feitas por outras comunidades como SSAC que é o comitê consultivo de segurança e estabilidade, e outras equipes de revisão, como a equipe de revisão de segurança, estabilidade e resiliência dois... Uma coisa que é muito interessante, que é muito difícil diferenciar questões de abuso técnico como phishing, botnet, malware, ido abuso do conteúdo, porque há muita sobreposição em diferentes tipos de abuso, como por exemplo, ou mais de um exemplo nesse estudo, mas uma fala sobre phishing, phishing pode envolver um registro malicioso, que diz: clique nesse link.

Isso leva a sites que tem conteúdo malicioso, então não é só uma questão de abuso do DNS, mas também do conteúdo. Habilidades de um software, e haverá um webinar sobre domínios maliciosos e comprometidos. Vocês entendam a complexidade do ecossistema, e

como é que isso se relaciona dentro da ICANN, e o que que a ICANN pode fazer ou não.

Essa última observação que eu vou fazer antes de ouvirem o autor do estudo, algum dos achados interessantes para o especial, que novos gTLD's, são alguns dos grupos mais prometidos de TLD's, em termos relativos, se você olhar o primeiro gráfico, 3%, essa é a porcentagem do mercado de novos gTLD's, na verdade 6%, mas quando se vê os domínios sofreram violação, é muito mais alto esse número, é mais de 20%, e isso temos que levar em conta ao pensar nas rodadas de novos gTLD's, e os 41% de quase todos os nomes de abusos estão concentrado os nomes tradicionais.

Também observaram que ocorre abuso nos registradores e 5% dos registradores são responsáveis por mais de 40% do abuso de nomes de domínio. Também observaram que os registradores e profissionais de serviço que estão sendo vítimas, eles respondem rapidamente aos relatos de abuso, e tomam medidas roídas e decisivas para reduzir o impacto. São importantes esses relatos, que muitos desses registradores são seriamente comprometidos, então eu gostaria de passar para Ivett que fez foi o estudo para Comissão Europeia, muito obrigada por ter aceitado participar e estamos aqui esperando a sua apresentação.

IVETT PAULOVICS:

Muito obrigada por me receberem, por uma questão de tempo, eu vou passar diretamente para minha apresentação, então vou falar dos objetivos do estudo que foi encomendado pela Comissão Europeia, a

metodologia, o cronograma, definição, que propusemos para abuso de DNS, a magnitude medida, as boas práticas identificadas, e as recomendações.

Os objetivos desse estudo eram muito amplos, foi pedido que avaliássemos fenômeno de abuso do DNS, a sua definição quais eram as tecnologias, papel dos atores, e avaliar a magnitude desse fenômeno, dar uma visão geral das normas, e na União Europeia e Global, e as práticas do setor, e encontrar boas práticas que nos ajudem, que são utilizadas, por intermediários, ou na ICANN ou de forma internacional, e as medidas necessárias para tratar disso. A metodologia que utilizamos então fizemos uma pesquisa ilegal com medidas em tempo real, pesquisas, entrevistas detalhadas, oficinas com participação de muitos especialistas, e durante a medição em tempo real, analisamos ao redor de 2,7 milhões de incidentes, e 1,68 milhões de nomes de domínio dados, usando as listas de domínios ou de URS, e depois fizemos uma revisão de relatórios de terceiros, esse estudo...

Esse foi o cronograma, fizemos as medidas no segundo trimestre de 2021, quanto à definição de abuso do DNS, isso a Laureen já mencionou, a limitação sobre as diferentes terminologias utilizadas, com sobreposições, portanto é difícil distinguir entre conteúdo técnico, ameaças de tipo técnicas, ameaças relacionadas a conteúdo, nossa proposta, é utilizar uma definição então mais ampla é o abuso do DNS, qualquer atividade que utilize nomes de domínio, ou protocolo do DNS, para atividades prejudiciais ou ilegais, nossa abordagem é de baixo acima, e para analisar cada incidente, o mais importante, essa

abordagem que distingue entre nomes de domínio registrados maliciosamente, nomes de domínio comprometidos, aqueles que são acreditados por registrantes ilegítimos, legítimos, mas que depois ficam comprometidos por criminosos.

Como categorizar o abuso do DNS, há três categorias, tipo um, são abusos relacionados a nomes de domínio registrados maliciosamente, tipo dois abusos relacionados a operação do DNS, e outras infraestruturas, e o tipo três, abusos relacionados a nomes de domínios que distribuem conteúdo malicioso. E é importante destacar que esse terceiro tipo aproveita nomes de domínio comprometidos ou registrados maliciosamente. Essa abordagem é importante também para distinguir entre os registrados maliciosamente, tipo um, e os maliciosos, isso nos leva a pergunta de quem deve resolver isso.

É a primeira categoria, tipo um, os nomes genéricos agora (inint) [00:21:38] para diferentes comunicações, e isso deve ser resolvido em nível do DNS, os intermediários devem agir no nível do DNS, e o conteúdo malicioso pode ser destruído utilizando nomes de domínio comprometidos, por exemplo os de (inint) [00:22:07] que servem conteúdo de phishing, enquanto a solução deve ser feita em nível do holsting, e também do DNS. E nisso é porque mitigar esse tipo de abuso só no nível do domínio não é eficiente.

Quanto ao conteúdo malicioso distribuindo utilizando nomes de domínio comprometidos, como aqueles que servem conteúdo de phishing tipo três, não é útil a resolvê-los, em nível do DNS, porque pode prejudicar o registrante legítimo, também os usuários que a solução

seja feita através do holsting, quanto a abusos relacionados às operações do DNS, isso eles devem ser resolvidos em nível do DNS, isso de acordo a nossa definição, que inclui também quem deve resolver esses abusos.

Quanto à magnitude dos abusos do DNS, um dos gráficos do estudo é esse aqui em que medimos a saúde geral dos TLD's, também vis a vis, os domínios abusados, comprometidos, também, reputação de registrantes e outras questões. Quanto à saúde geral dos TLD's, como disse a Laureen, neste gráfico, vemos a distribuição que compara a participação de mercado de diferentes grupos, e a sua distribuição. Distribuição de domínios, de todos os domínios, os abusados, e concluímos que os ccTLD's são os menos submetidos a abusos, em termos relativos ao vis a vis no mercado. 14,44% de participação de mercado e menos de 1% dos ccTLD's abusados.

Laureen já mencionou gTLD's, 6,6% dos novos gTDL's, e os resultados mostram que nem todos os novos gTLD's, passam por abusos. E aqui vemos também a distribuição dos nomes de domínio comprometidos em azul, e os registrados maliciosamente em vermelho por tipo de abuso, 25% por exemplo, que padeceram, phishing, e a maioria passou por malware, aqui vemos a distribuição dos nomes de domínio comprometidos e registrados maliciosamente, por tipo de TLD, vamos para o próximo, e como eu disse, aqui o que importa é a reputação do registrer, também do provedor de holsting, e os principais registres mais abusados, representam 48% dos nomes de domínio registrados maliciosamente, também, observamos concentrações desproporcionais nos domínios PAM que alcançaram domínios

abusados, três mil domínios abusados por cada 10 mil nomes de registro e a adoção de sanções de segurança DNS, protocolos de proteção de e-mails.

E por último, depois de ter analisado todas as políticas aplicáveis em nível internacional e da União Europeia, e também algumas sobre regulações, identificamos as boas práticas dos diferentes tipos, identificamos 55 dessas boas práticas, com transparência, informação, do tipo reativo, preventivo, com intermediários, vemos aqui algumas amostras, de ccTLD's, alguns exemplos também de registros de gTLD's, e eu não tenho muito tempo para entrar em detalhes, mas queríamos todas essas práticas, e esse estudo analisa tudo isso bem em detalhe, e por último nesse estudo identificamos uma série de 27 recomendações em seis áreas para melhorar as medidas de mitigação de abusos do DNS.

Não posso mencionar todas as recomendações, essas 27 claro, mas algumas que são técnicas, algumas vinculadas às políticas e que também tratam sobre diferentes intermediários para (inint) [00:29:00] e revendedores, recomendações um serviço padronizado centralizado para o registro de abusos para verificar os casos de registros de nomes de domínio e através do seu cliente, para usar isso em algoritmos preditivos e monitorar as taxas de abuso, e também para utilizar, para determinar patamares.

E também identificar recomendações similares de taxas de abuso que não ultrapassem alguns limiares determinados e quanto ao último esforço de colaboração em nível da União Europeia Recomendamos

harmonizar as operações de CTLD's adotando as boas práticas e identifica-las também para colaborar com as instituições, órgãos governamentais, quanto a identificadores confiáveis há uma série de recomendações, como disse a Laureen, que também pode ser observados com diferentes tipos de estudo, mas esse estudo tentou apresentar uma visão geral do fenômeno que observamos em 2021, esse meu último slide aqui, vocês... Aqui tem os links para fazer download do estudo, também entrou em contato comigo, ou também com a Maciej da Universidade de (inint) [00:31:07] que não conseguiu estar aqui, ela está participando da sessão dos grupos empresariais aqui da ICANN. E obrigada pela atenção.

LAUREEN KAPIN:

Obrigada, eu sei que a Manal sugeriu algumas perguntas aqui no chat, e vamos fazer uma pausa para aqueles que têm perguntas principalmente sobre o estudo, há muito ainda para mencionar sobre isso, temos uma pergunta do Finn, a Gemma... O Finn perguntou se há alguma solução fácil e rápida, quanto à recomendação que seja fácil de aplicar, fácil e rápida de aplicar. E acho que essa pergunta é para você Ivett.

IVETT PAULOVICS:

Sim, obrigada, não é uma pergunta fácil, esse estudo foi encomendado pela Comissão Europeia, portanto, para a Comissão Europeia poderia ser mais fácil ter acesso aos ccTLD's, para harmonizar as operações dos ccTLD's, e através da ação das boas práticas, mas na ICANN, talvez haja outras prioridades. Outras recomendações, que poderiam ser adotadas

mais facilmente, porque há outros modelos que existem para a ICANN, ou trabalhos paralelos.

ESTADOS UNIDOS:

Realmente apreciamos muito esse estudo de abuso que precisam ser muito abrangentes, para os registradores e também para entender as áreas comerciais e técnicas, sob o ponto de vista legal na internet mas a definição de abuso do DNS é que talvez seja excessivamente ampla nesse estudo né? E isso para ser usado na ICANN é amplo demais e pode ser prejudicial isso na internet, mas nós achamos que esse é o espaço ideal para facilitar uma troca de ideias sobre esses problemas entre os especialistas de governo e as políticas do DNS e reconhecemos que pode ser muito útil e reconhecemos que sobre essa definição tanta de abuso do DNS, sim, essa definição poderia ser aplicada para a ICANN e também fora da ICANN.

LAUREEN KAPIN:

Obrigada Susan, a próxima é a Gemma.

GEMMA:

Espero que estejam me ouvindo bem, eu tive... Eu assisti esse tema em outra sessão. Então eu acho que nossos... Não foi bem divulgado, e às vezes é difícil ter um diálogo com a comunidade da ICANN, então muito obrigado Ivett pra sua apresentação, e como a Laureen mencionou no início, também teve uma apresentação no PSWG, e eu fiquei muito impressionada com o resumo que a Laureen fez no início, porque de fato há coisas que são discutidas no PSWG, que podem ser respostas à

pergunta do Finn, de coisas que podem ser aplicadas imediatamente nos contratos da ICANN quanto abuso do GNS e isso tem sido discutido na ICANN, foi tema de assunto depois do relatório do SSR2.

Eu gostaria de dizer em primeiro lugar a nossa abordagem, que o nosso estudo é independente, que nós encomendamos para especialistas fora da comissão europeia, e eu diria sem um prazo específico para uma elaboração de política, na verdade essa é uma questão comercial importante para nós. E centrado para estratégia de cyber segurança da Comissão Europeia, eu gostaria que houvesse de falar que esse espaço dado para esse tema, nós continuamos na dizer que a ICANN é o lugar onde o abuso do DNS deve ser discutido, então nós queríamos dar a maior visibilidade a esse estudo na agenda da ICANN, e em diferentes grupos constitutivos.

Mas esse é um estudo independente, não é uma bíblia, então alguns elementos devem ser modificados, eu acho que comentários são bem vindos, mas isso de forma nenhuma é um estudo sobre a (inint) [00:38:18] então é a segunda ou terceira vez que esse estudo é apresentado. Então, o que que a ICANN pode fazer? Bom, isso é fora do mandato da ICANN, todos na comunidade estão interessados em implementar medidas contra o abuso do DNS, como a Ivett apresentou, isso não termina ou começa com o registro de domínios malicioso, pode haver impacto, mais tarde e afetar outros atores.

O que nós temos que pensar, no abuso do DNS de forma holística, nós estamos olhando o abuso do DNS do lado das vítimas então, quais são as controvérsias em relação, o que é exatamente o abuso do DNS, não

é essa questão, é isso que está acontecendo, e isso está acontecendo através do DNS, pelo registro de domínios maliciosos, esse estudo claro, é muito longo, eu acho que ele não pode ser apresentado como um todo nesse texto, mas eu sei que é um ambiente muito complexo com registro, registradores e distribuidores.

Então e quanto aos provedores de hospedagem, e em que nível acontece o abuso, então os atores tem a capacidade de informar uns aos outros o que está acontecendo. Então o que é mais... O que está pronto (inint) [00:40:35] o que está acontecendo. E isso pode fazer muita diferença, então garantir que alguém seja responsável dentro da organização e garantir que os atores possam se comunicar, então nesse ponto é muito importante termos registros do WHOIS bastante precisos, eu sei que esse tema é bastante extenso, mas o que eu gostaria de dizer é: a comunidade da ICANN, vai utilizar, há várias coisas que são uteis, então o que esse estudo mostra é o que nós na Comissão Europeia podemos fazer.

Nós queremos saber se a comunidade acha alguma coisa útil, e podemos aliar se foram feitos, se alguma coisa melhorou. Eu acho que pé importante focar no que é possível fazer, e não concentrar no que a ICANN pode fazer ou não. Muito obrigado Laureen, desculpe pela intervenção tão longa, mas eu achava que era importante esse esclarecimento.

LAUREEN KAPIN:

Muito obrigado Gemma. Será que Manal, a gente pode ter mais alguns minutos já que os comentários foram tão bons? Você não precisa

responder agora, nós vamos voltar aos slides, e vamos reorganizar um pouco, então eu pediria para pedir para passar direto para o meu colega do Japão, para fazermos, mostrar um pouco do restante do material, então eu passo a palavra para o colega do Japão, Sumitaka Shirakabe, do Japão.

SUMITAKA SHIRAKABE:

Muito obrigado Laureen. Muito obrigado pela oportunidade e eu sei que há pouco tempo, eu quero compartilhar os meus slides rapidamente, então na última reunião do GAC, na ICANN 72 compartilhamos a questão do hopping, em pular de um registro em que um registrante continua o alvo, transferindo o mesmo nome de domínio de um registrador para outro, e nós gostaríamos de compartilhar um caso em que o registrante parece ser o mesmo e continua violações usando diferentes nomes de domínio, registrados sob o mesmo registrador, e esse é meu ponto de vista sobre o Japão, e foram sugeridos dois pontos, o primeiro é garantir o cumprimento entre a ICANN, registro e registrador como meu colega mencionou.

É importante coletar informações diretas dos registrantes no momento do registro do domínio e garantir a exatidão das informações. E também é importante fazer a auditoria eficaz, e continua sobre a compliance dos registradores aos (inint) [00:45:24] da ICANN e quais são as medidas contra o abuso do uso de domínios, consideramos a possibilidade de usar um programa de notificação confiável especialmente no caso de abuso de conteúdo e sugerimos que a cooperação e a discussão com outros OA's e IC's dentro da ICANN na

reunião da ICANN 72, houve uma discussão quanto ao abuso do DNS, do GAC com ALAC, e isso resultou na formação de um pequeno grupo, essa era uma das ações, e hoje de manhã, mencionado pelo CCNTO, temos uma ajuda proativa de ações, e esperamos uma maior colaboração do GAC com outros grupos como os colegas já mencionaram, sabemos que o mandato da ICANN é limitado, mas precisamos ser mais proativos.

LAUREEN KAPIN: Muito obrigada, muito obrigada Sumitaka por sua apresentação.

MANAL ISMAIL: Laureen, desculpe interromper, agradeço Sumitaka, e então nós conseguimos mais 10 minutos com a Luísa, então você pode então falar até 16:25.

SUMITAKA SHIRAKABE: Então eu pediria que voltasse alguns slides, um a mais aí... Eu vou passar a palavra então a Gabriel, para que mostre brevemente o restante do material.

GABRIEL ANDREWS: Muito bem, então eu queria dizer que foi muito interessante o estudo que foi apresentado, mas eu queria mencionar um importantíssimo estudo do grupo de estudos técnicos, de iniciativas de facilitação de segurança do DNS, em resposta aos ataques como os que ocorreram em 2018, como o (inint) [00:49:00] e o DNS espionagem, então esse grupo

de estudos viu não só esses ataques, mas outros também utilizou exemplos e propuseram melhores práticas, para tratar esses incidentes globais.

Então todas recomendações foram enviadas para o diretor de segurança da ICANN, talvez a ICANN responda, mas não é necessária nenhuma ação imediata da ICANN, vocês devem lembrar que em 19 de março de 2021 o SSAC publicou os (inint) [00:50:01] um relatório sobre tratar o abuso, e tinha uma recomendação que falava da criação de um facilitador comum em resposta ao abuso.

E temos um possível candidato, e a esse instituto de abuso do DNS, que foi criado por um registro que estão criando uma ferramenta centralizada de relato de abuso ou de denúncia de abuso CAT, que deve começar a ser testada em março talvez seja lançada em junho, então normatiza o roteamento das queixas de, o encaminhamento das queixas de abuso, e melhora os informes, esperamos ver quais resultados, então quanto às outras iniciativas, a GNSO criou recentemente um pequeno grupo sobre abuso do DNS, e começaram a compartilhar perguntas inclusive ao GAC, para entender melhor quais são as expectativas do GNS, e se outra, elaborar mais normas contribuía para as iniciativas que já existem, então se espera uma resposta até no dia 21 março nós convidamos o GAC a fazer uma contribuição até o 21 de março. E finalmente amanhã, haverá uma plenária, sobre domínios registrados maliciosamente ou como encaminhar as denúncias de abuso, esse painel vai lidar exatamente com isso.

Então com isso eu passo a palavra de volta, a Laureen, são domínios comprometidos, e domínios vítimas de abuso. Então com o trabalho futuro, eu gostaria de destacar, queremos continuar a trabalhar e melhorar as exigências do contrato, e temos um texto no último communicate que os estatutos autorizam a ICANN a negociar os contratos, então nós achamos que pode ser feito junto com as partes interessadas da ICANN para melhorar as cláusulas do contrato para responder melhor o abuso do DNS, e outras avaliações do abuso do DNS, e especialmente pelo comitê do SR, recomendou então o estudo das causas, etc., para a próxima rodada de novos gTLD's, antes de lançar uma nova rodada, é sempre bom saber o que nós já temos, então me desculpem que não tenhamos mais tempo para perguntas que certamente vocês gostariam de fazer, então vocês podem entrar em contato com nosso grupo, em qualquer momento e nós queremos conversar com vocês. E então eu vou passar para Manal.

MANAL ISMAIL:

Muito obrigada Ivett Sumitaka, e Laureen, agradeço Fabien ao seu apoio, e então vou passar agora para os procedimentos subsequentes.

[FIM DA TRANSCRIÇÃO]