HYDERABAD – Sessão de Tópicos de Maior Interesse: Mitigação de Abuso em gTLDs
Sábado, 5 de novembro de 2016 – 13h45 às 15h IST
ICANN57 | Hyderabad, Índia

DESCONHECIDA: Essa é uma questão de auto interesse, de mitigação e abuso gTLDs 5 de novembro de 2016, das 13:45 às 15 horas.

ALICE MUNYUA: Boa tarde para todos, essa é uma sessão muito interessante, organizada pelo comitê consultivo governamental, eu sou Alice Munya, do Grupo de Segurança dentro do GAC, e eu vou começar com uma apresentação rápida dos painelistas aqui, por favor, digam seus nomes e grupo.

MICHELE NEYLON: Michele Neylon, dos ajustadores, eu sou consultor de registros.

BRIAM CIMBOLIC: Eu sou Briam Cimbolic, registros.

STATTON HAMMOCK: Statton Hammock, registros.

CARLOS ALVAREZ: C arlos da equipe da SSR.

ALLEN GROGAN: Allen Grogan de cumprimento.

DENISE MICHEL: Denise Michel de empresas.

DREW BAGLE: Drey Bagle.

BOBBY FLAIM: Bobby Flaim.

FABIEM BETREMIEUX: Fabiam Betremieux de apoio do GAC.

RICHARD ROBERTO: Richard do setor de registro.

ALICE MUNYUA: Muito obrigada, o grupo de trabalho foi criado em 2015 durante o encontro de Singapura, e vamos direto então para a sessão, não quero continuar com a história, e essa sessão vai se focar na

questão da mitigação de abusos de gTLDs e o que esperamos dessa sessão é fornecer informação atualizada à comunidade da ICANN ou às ICC's, sobre as melhores práticas da indústria para mitigar os abusos nos gTLDs. Também vamos atualizar informações sobre a situação atual das atividades relevantes, inclusive compartilhando informações pertinentes, e também o trabalho que está ainda em andamento, e dar oportunidade para todos nós como comunidade da ICANN de conscientizar e apresentar pontos de vistas e especialmente tudo que tem a ver com opiniões e revisões das atividades atuais então vão começar com definição de Bobby Flaim sobre esse grupo de trabalho de segurança pública.

BOBBY FLAIM: Obrigado, quando falamos em abuso, e nós tivemos um juiz nos Estados Unidos que tentou descrever, ou definir a pornografia que acontece só quando a gente assiste, e isso acontece também com o DNS quando a gente usa mal o DNS. O abuso do DNS, e desse grupo de trabalho surgiram a salva guardas que para proteção de phishing, de malware, e de outras formas de abuso, e essas formas de abuso dependem de cada país, e cada país tem seu direito, sua legislação, mas existe essa exploração do DNS, abusos de crianças, terrorismos, e outras questões que já observamos, já assistimos na TV, não há então uma única definição de abuso do gTLDs, então devemos considerar sim

uma coisa na hora da pensar na segurança pública do DNS que é, e lembramos de tudo isso. Então nós devemos, como (inint) [00:05:06] os registradores, operadores, etc., sobre cumprimento da lei, e ver o que tem sido feito, as melhores práticas para prevenir e mitigar os abusos. Estamos muito confiantes de que essa vai ser uma reunião produtiva, muito útil e informativa, e não só aqui dos painelistas, mas também dos painelistas com o público, eu vou apresentar aqui o meu colega Drew, quem vai falar um pouco sobre alguns exemplos de abusos, obrigado.

DREW BAGLEY: Obrigado Bob, eu vou falar a perspectiva de algumas tendências de abusos que vemos na fundação de segurança do DNSQ, uma organização em fins lucrativos, e o abuso do DNS é importante, e não apenas dentro do contexto da ICANN, mas também no mundo, considerando as vítimas das últimas tendências do cyber delito. Muitas manchetes que vemos hoje começam com o termo registro de nome e domínios. Então as definições de abuso nos levam a pensar em phishing, em botnet, e esses temos, mas há outros, eu agora vou concentrar-me nesses que eu mencionei. E uma tendência que muitos conhecem dos últimos anos, é o abuso do DNS, e com ramificações financeiras enormes. Antes eram casos isolados, vítimas isoladas, eram delitos de pequena escala, mas hoje os abusos afetam a

estabilidade de todo o sistema DNS. Uma das últimas tendências especialmente no último ano, e algumas das notícias mais recentes, são os ransomware, com que comprometem os e-mails, e e-mails comerciais, e comprometem também a internet das coisas, o ransomware, começou também a pequena escala com indivíduos que eram vítimas quando clicavam num link, seu computador ficava criptografado, e sequestrava de uma maneira, mas agora isso acontece em grande escala, nas empresas, em grandes empresas, hospitais também, por exemplo, e dessa maneira, uma empresa pode perder instantaneamente, tudo que tem a ver com confidencialidade, e isso pode ser resolvido se eles pagam um resgate, e uma das últimas estatísticas, demonstra que essas infecções aumentaram rapidamente neste ano, último ano, houve muitas infecções, em que houve 23 infecções por mês. E a quantidade de dinheiro que houve foi altíssima. E outra tendência é, e hoje há um serviço para resolver o ransomware, e agora nós também podemos executar o ransomware, e pagar também o comprometimento dos e-mails, que isso implica uma engenharia muito cuidadosa na internet, que atinge executivos de negócios, por exemplo, e em última instância, isso é resolvido através de uma transação financeira em que no executivo pensa que ele está recebendo uma solicitação legítima do departamento contábil da empresa onde ele trabalha, e isso implica perdas enormes de bilhões de dólares. Também o

botnet da internet das coisas, nós já vimos isso nas últimas semanas, nos ataques para o DYN, e também cyber ataques na Libéria, e infelizmente não tenho mais tempo para descrever isso, mas há muitos ataques para os nomes de domínios, e é importante então recorrer à registros que ofereçam esses sistemas de proteção de privacidade e proxy. Os registradores de registros são responsáveis, e não devem recorrer aos revendedores. Há uma tendência muito interessante, em termo de que afeta uma das maiores tendências o cyber delito agora.

BOBBY FLAIM: Eu gostaria de fazer uma pergunta, baseado na tendência que vocês veem ameaça o DNS e Bitcoin, qual você acha que seria uma solução pra essas ameaças?

DREW BEAGLE: Eu acho que uma das principais soluções, seria a mitigação, anti abuso proativa, essencialmente quando não se tem bons dados para se trabalhar, ou credenciais falsas, há dados incomuns, porque esses falsários precisam aumentar a escala, como todos os outros. Então tem havido uma certa pressão dos provedores de proxi, e há evidências para compartilhar dados, e também se pode impedir os registrantes que estão cometendo esses abusos.

ALLEN GROGAN: O departamento de cumprimento contratual de alto nível da ICANN, fiscaliza os contratos que temos com os registradores e registros. Como esta é a primeira reunião pós transição, eu gostaria de falar do marco de referência, eu não vou tentar responder a pergunta, eu só vou tentar definir a pergunta. Então sobre os novos estatutos e missão, é uma das proibições da ICANN ir além da sua missão, e essa missão é técnica e está relacionada à coordenação, facilitar o sistema de zona raiz, sistemas autônomos, sistemas de protocolos, então o uso de identificadores únicos da internet, ou o conteúdo desses serviços não é parte da missão da ICANN, mas na minha abertura eu falei dos contratos, há uma cláusula quanto aos acordos antes de 1º de outubro de 2016, então os nossos contratos são basicamente os mesmos, e haverá renovação desses contratos, como eu mostro aqui nesses slides várias cláusulas que estão nos nossos contratos quanto ao abuso. E ao pensar nisso e qual é o papel da ICANN, no combate ao abuso, lembre-se que independente das nossas ações, devem estar dentro do escopo dos estatutos e da missão, e devem estar nos contratos. E eu vou passar então pro Carlos Alvarez pra falar sobre o restante desse assunto.

CARLOS ALVAREZ: Eu sou membro da equipe de resiliência, estabilidade e segurança, estamos trabalhando com a segurança, a comunidade de segurança, o nosso enfoque não é o contrato, isso é o Allan que faz, mas o nosso enfoque é cooperação voluntária para monitorar atividades relacionadas a botnet, phishing, são atividades maliciosas, então a gente não trabalha com questões coorporativas, marca registrada, o que nós trabalhamos é só com isso, para deixar isso bem claro. Eu gostaria de deixar aqui, mostrar aqui algumas coisas que nós fazemos, que vale a pena mencionar, e uma delas que fazemos sempre, é treinar as forças policiais através do mundo, todas as semanas alguém da nossa equipe vai a algum país e em suas regiões para treinar a polícia desde o fundamental do DNS até investigações detalhadas, e o que pode significar uma ameaça ao sistema do DNS como um todo. Como um exemplo, fizemos já vários treinamentos nos Estado Unidos, no DOJ, Cybersecurity Center, também na Europa, no Oriente Médio, na América Latina esse ano, estivemos em vários países, duas vezes no Peru, na Colômbia, alguns exemplos, nós damos apoio da comunidade operacional de diferentes formas, fazemos recomendações quanto às investigações que estão em andamento, que tem a ver com recursos do DNS não quero saber o que eles estão investigando, só dizemos como é que o DNS funciona. Nós temos que, queremos que eles entendam quais são as cláusulas contratuais, qual é o marco dos contratos. Então quais são os

passos que eles podem utilizar para enviar informes sobre abuso, então nós ajudamos os colegas das forças policiais quando eles tem solicitações, quando eles fazem uma solicitação rápida de segurança, é um processo muito bom e eficiente da ICANN, por exemplo, foram botnets que foram Cryptlocker, e o Game Over que aconteceram em pouco tempo, e nós fazemos recomendações à equipe, e comunidade, exemplos atuais, são o marco de segurança mundial de registros, e se vocês tiverem perguntas em relação a questões de SSR, Segurança, Estabilidade e Resiliência. Quais são os desafios? Há registros com diferentes sistemas, processos, disponibilidades de recursos e níveis de especialização, às vezes os informes de abusos não são claros, não dão informações suficientes, às vezes há falsos positivos, e não há uma padronização do informe de abusos, e isso aí complica as coisas em termo de controle de fiscalização. Então às vezes há falta de entendimento tanto do lado de quem faz a queixa, e de quem recebe a queixa, o que vale a pena mencionar também que não dá um termo de serviço padrão. Então alguns registradores têm termos de serviços mais rígidos, outros são mais lenientes, então não há uma uniformidade, e é complicado também conseguir dados para a pesquisa. Antes de ter uma definição mais clara, do que abuso do DNS, então talvez outros, da comunidade, podem ajudar-nos a definir isso, para incluir no

modelo da ICANN e para a padronização dos processos. Bom, e isso era o que eu tinha pra dizer, muito obrigado.

BOBBY FLAIM: Obrigado Carlos, eu gostaria que o Drew falasse, e ele quer falar sobre soluções de abuso do DNS.

DREW BEAGLEY: Muito obrigado, eu gostaria de enfatizar que além do papel da ICANN, e de outras partes, é importante que os registradores e registros compartilhem essas informações uns com os outros diretamente, ou através de uma outra instituição, isso é muito importante, e esses dados em comum, que são compartilhadores pelos veladores, existem então só compartilhando essas informações é que vamos conseguir combater esses crimes e a mensagem que é, nós temos diferentes partes da comunidade que podem ver o que podem fazer com os dados que tem para ajudar uns aos outros, para tornar a internet mais segura. E isso eu acho que ocorre através da cooperação.

BOBBY FLAIM: Perguntas pra Allan e Carlos vocês acham que agora após a IANA, nós entramos num período em que vai ser possível ter ações mais proativas em termos de segurança?

ALLAN GROGAN: Eu não sei exatamente o que você está perguntando, você pode detalhar?

BOBBY FLAIM: Bom, agora num mundo pós a IANA, a ICANN é independente, vocês acham que a comunidade pode buscar, pedir que vocês façam mais em termos de autocorreção, auto regulação, de controle dos contratos, agora que não há uma supervisão, entre aspas.

ALLAN GROGAN: Eu acho que no pós-IANA, haverá muita discussão na comunidade sobre qual é o papel da ICANN no combate de abusos, e eu não tenho certeza de qual é a direção que a discussão vai tomar, diferentes partes da ICANN tem diferentes pontos de vista. Quanto ao mandato e a missão da ICANN em relação à isso, à essa mudança da missão e dos estatutos depois no pós IANA, eu acho que vai haver muito debate, muita gente vai pedir que façamos mais e outros menos.

CARLOS ALVAREZ: Os nossos colegas de operações e forças policiais que eles gostariam que a ICANN fosse mais ativa, contra o abuso, então eu acho que a comunidade da ICANN, deve determinar qual deverá ser a sua contribuição nisso.

BOBBY FLAIM: Obrigado, agora temos Statton e Brian que vão falar, nos representar ou discutir melhores práticas de mitigação de abuso do DNS.

BRIANM CIMBOLIC: Eu sou representante dos registros, nós temos um programa de abuso, que começa e termina com políticas anti abuso. Que cobre desde questões técnicas até exploração infantil, e nós temos algumas medidas proativas e reativas para mitigar o abuso. Quanto às ativas, nós temos um abuso nesses sites, então isso é monitorado 24 horas por dia. 365 dias por anos, e há um conselho geral que vai determinar qual é a atribuição para quem enviar a investigação. Então em 8 a 12 horas há uma resposta, em geral os usuários finais ou policiais entram em contato, a maior parte de usuários final, eles querem que intervenham no nome de domínio, que inspirou e que outras pessoas registraram, e isso não está dentro do nosso mandato. Em geral o que é relatado é spam e phishing, e fonte da industrial em geral é mal, quando há um verdadeiro abuso, isso é passado pro registrador, porque nós levamos em conta a relação que o registrador tem com o seu registro, e nós pedimos então uma explicação por que, que está acontecendo esse spam, ou etc. O que os registrados em geral, por nossa

recomendação, suspendem os domínios, e às vezes dizemos: “se você não agir, nós vamos usar apolítica anti abuso e vamos suspender o domínio”, e geralmente suspendemos o domínio, porque as deleções, não funcionam quando o nome de domínio é delatado no dia seguinte ele é registrado pelo mesmo indivíduo com o mesmo objetivo de abuso. Quanto às forças policiais, as solicitações das forças policiais, nós temos mais ação e então, inclusive ajudamos a estabelecer que tipo de texto se pode utilizar em termos jurídicos, também implementamos medidas proativas, e essa área nós utilizamos bastante com o usuário final, por exemplo, se um registrador tem um pico muito alto nos registros diários, nós damos uma olhada. Não significa que todos os registros são abusos, talvez seja um dia bom para esse registrador, mas isso nos dá razão para investigar melhor, para ver se há abuso ou não, se é spam ou outra coisa. E nós temos um relatório diário dos registros do dia e fazemos uma referência cruzada, com o WHOIS. Isso não significa que necessariamente há abuso, nós devemos ver os registros para ver se não há algo estranho acontecendo, e no caso de haver abuso com essas medidas proativas, nós utilizamos as medidas reativas, nós contratamos o registrador, fazemos com que ele contrate o registro, o registrante, e se for o caso, o nome de domínio é suspenso, e com isso eu passo então de volta pro Statton.

STATTON HAMMOCK: Namastê a todos, muito obrigado, Statton Hammock, sou do Rightside, são os serviços de domínio verticalmente integrado, somos registro e registrador. Operador de registros pelos quatro nomes de domínio principal, e somos um distribuidor de nomes de domínio. Como vice-presidente de políticas e de questões jurídicas nós temos uma janela muito grande para dados relacionados a abuso, tanto do registrador coimo do registro, e nós podemos compartilhar isso. em primeiro lugar quando se fala de abuso, eu gostaria de deixar claro que quando fala de medidas anti abuso, são várias coisas diferentes, algumas são demandadas pelos registros, dentro do contato com a ICANN como mecanismo de proteção de direitos que foram desenvolvidos durante a elaboração do novo programa dos novos gTLDs, como Sunrise, processo de resolução, processo de resolução de disputas, também como registros, nós tivemos que incluir compromissos de interesse público, alguns foram demandados pela comunidade multisetorial, outros por recomendação do GAC e outros foram implementados dentro dos nossos contratos de registro. E há esforços voluntários que não são contratuais, que os registros, registradores utilizam para combater atividades nefastas na internet. Então o Rightside, oferece uma lista de domínios bloqueados, e então, para que os registros não gastem um montão de dinheiro

pesquisando os gTLDs e nós temos um processo de queixos bastante longo, de 90 dias, para alertar que há infração da marca registrada, e também há atividades para criar um marco de segurança nos quais os membros dos grupos de registros, estão trabalhando. E há várias outras atividades voluntárias dentro da comunidade da ICANN em que registradores e registros, estão tentando então evitar diferentes tipos de abuso, e alguns têm a ver com abuso infantil, outros direitos, copyright ou direitos autorais, outro uma iniciativa de nomes de domínios saudáveis, outros tem melhores práticas para impedir a venda ilegal de medicamentos, outras para contra-ataques a segurança. Isso é mais ou menos o que acontece em termos de atividades anti abuso. Nós temos mais de meio milhão de domínios nas nossas quatro gTLDs, nós teremos três fontes de relatórios de abusos, são altamente regulados, são .LAWYER, nomes profissionais por exemplo, são altamente regulados, .DENTISTA, há disputas, nós temos procedimentos para resolução de disputas, então os dados aqui à direita mostram as atividades em todos registros, e vemos que isso é consistente com a exigência de cumprimento dos contratos da ICANN em termos de abuso, maior parte são phishing, malwares e SPAM que se espera pouco sobre conteúdo, ou queixas que achávamos que aconteceriam nos domínios de topo. Em resposta à essas queixas, algumas ações são tomadas pelo registrador, outras pelos registros, para então destacar devido

ao número de nomes de domínio registrados, há baixo nível de abusos, e esse slide mostra à direita, e o meu colega Brian aqui, me ajudou a montar esse slide muito obrigado.

BOBBY FLAIM: Muito obrigado Statton e Bryan, eu gostaria de pergunta, vocês compartilham as informações sobre abuso, se vocês veem alguma tendência ou certos atores?

STATTON HAMMOCK: Sim, informalmente nós fazemos, sou Statton do Rightside, a minha equipe de conformidade compartilha informações com outros registradores demais atores, se alguém está tentando sequestrar algum nome, ou utilizar para alguma atividade nefasta, isso é compartilhado com outros registradores. Mas não há nada formal, isso é feito como uma boa prática.

BOBBY FLAIM: Obrigado Statton, nós temos Giovani Seppia, perdão, desculpa, eu não consigo ver todos.

NÃOIDENTIFICADO: Uma pergunta, eu sou (inint) [00:35:47] um membro da ICANN e também membro do comitê NomCom, tenho uma pergunta sobre fonte e blocos de listas, e são perguntas sobre PIR por

exemplo, você faz um scan dos seus relatórios através de várias fontes de listas negras, de onde é que você colhe isso? Desculpa.

BRIAN CIMBOLIC: Bom, temos uma lista pública, quem quer responder a pergunta, temos uma lista pública altamente sensível, e uma das maneiras em que nós tentamos mitigar possíveis problemas, é pelo caminho que nós tomamos de referência, e muitas vezes aproveitamos essas informações, essas oportunidades para chegar a conclusão de que alguma coisa, que há um abuso, e continua, quem pergunta, eu vou assumir que essas listas são a fonte, uma fonte verificável em geral né? Sim, essa é uma fonte verificada.

BRIAN CIMBOLIC: Eu acho que poderíamos deixar as perguntas para o final de todas as apresentações, porque é preciso termos primeiro as apresentações, e depois teremos 30 minutos aproximadamente para o debate, perguntas e repostas.

KIRAN MALANCHARUVIL: Como acompanhei a proteção de marcas e recebi muitas notificações de abusos de marcas, e acho que não é necessariamente justo dizer que porque não denunciamos

abusos, não significa que não haja abusos ou que haja abusos em outras partes. E acho que as políticas de abusos não são muito extensas, são bem estreitas, e é por isso que muitas vezes não recorremos à essas denúncias na nossa indústria, então seria muito bom que vocês nos deixassem entender quantos nomes de domínios são denunciados através de ISP's e registradores, etc. Acho que esses seriam dados mais sérios, para ver que tipo de abusos são denunciados, e não aqueles que são denunciados a vocês como registros.

STATTON HAMMOCK: Sim, eu concordo, muitas vezes o registro chega, de uso indevido, o departamento da ICANN…

BOBBY FLAIM: Vamos passar para Giovani.

GIOVANNI SEPPIA: Agradeço a oportunidade, Giovanni Seppia, gerente externo de .EURid, e isso é para destacar que do ponto de visto técnico e administrativo o registro .EURid de ccTLDs, nós pertencemos à família dos ccTLDs, estamos altamente regulados, temos as regulações da União Europeia de 2002, e uma segunda parte de regras de políticas de2004. Os dois conjuntos de regulações, contém uma cláusula segundo o .DOT não é apenas para a União Europeia Econômica. Nós estamos servindo um Mercado

de 31 países, temos mais de 3.8 milhões de nomes de domínio, e desde 1º de junho deste ano temos também a escrita cirílica, e é importante destacar que nós temos esse aspect multilíngue. Implementamos uma série de medidas para proteger os nomes de domínio do ponto de vista administrativa, temos o DNSSEC, o lock de registros, depois temos o bundling e temos a combinação de escritas. Temos então esses bandos ou conjuntos de homoglifos, e dessa maneira protegemos os titulares de nomes de domínio, de possíveis problemas vindos de nomes de domínio similares, que podem estar sendo registrados ou registrantes. E também lançamos o .DOT em idioma cirílico, que é um nível implementar de segurança, para o nosso ambiente. E o que implementamos há alguns anos, é o plano de qualidade de WHOIS, a autoridade do registro .DOT está muito limitado por essas duas regulações e, portanto, devemos operar quando for possível e dentro do marco dessas regulações, e agimos em geral quando recebemos queixas sobre possíveis abusos relacionados aos nomes de domínio da .EU. E isso temos desenvolvido em cooperação com os nossos registradores, e com om conselho de registradores, e para assim desenvolver um plano de qualidade. Isso para verificar os dados de registro, e principalmente verificar esses dados de maneira diária. Os dados de registro são verificados pela EURid, ou por terceiras partes contratadas, autoridades de aplicação de lei, e a verificação principal relacionada à essa verificação de

endereços, como o nome de domínio .EU, pode ser registrado pelos residentes de 31 países, e no final de 2015, nós eliminamos mais de 30 mil nomes de domínio .DOT porque não cumpriam com os critérios de residência conforme os critérios. Essa é uma lista ou as regulamentações. Essa é uma lista das autoridades que estão na Bélgica, nós temos um memorando de entendimento também com uma grande cooperação e diálogo, e alguns dos meus colegas, e meu, esse painel aqui menciona muito, a educação é preciso contratar muita educação para que os políticos ou pessoas de alto nível entendam e possam cooperar com os registros. E também temos o sistema de aviso, alerta precoce, por casos de abuso e altamente estamos desenvolvendo isso e trabalhamos em cooperação com as universidades (inint) [00:44:29] para prognosticar possíveis abusos e, portanto, demorar a delegação das solicitações de registro para aqueles nomes de domínio, então novamente isso pode levar a abusos e estamos apenas no começo, e devemos ver se podemos aplicar o princípio de prevenção, ao invés do princípio de remediação posterior. Eu fico aberto à perguntas, (inint) [00:45:03].

BOBBY FLAIM: Muito obrigado, eu tenho uma pergunta para você, vocês estão fazendo muita mitigação anti abusos e de, podem quantificar os recursos que vocês estão agora desenvolvendo?

GIOVANNI SEPPIA: Sim, boa pergunta, por que o que nós observamos durante os anos, é que bom, decidimos há alguns anos, que ter o ponto como domínio de qualidade, investimos muitos recursos para incluirmos todas as medidas possíveis para a prevenção e mitigação de abusos. Às vezes os departamentos jurídicos não, atualmente tem três pessoas dedicadas a estudar esses casos de abusos de domínio, a minha equipe cobre os países da União Europeia e ajudam a equipe dos jurídicos para entrar em contato com os registros. Também quero demonstrar aqui a importância de cooperação entre registradores de registros, e nós temos tido exemplos sim muito bons, nos últimos anos de ações, dos nossos registrantes, registradores, contra algumas das ações dos revendedores em casos de abusos, e de todo o registro. E esse é um elemento chave para o combate ao abuso.

BOBBY FLAIM: Como você trabalha efetivamente com os registradores, como é que vocês agem? Como vocês percebem, por exemplo, coisas que podem iniciar algum problema de abuso?

GIOVANNI SEPPIA: Bom, reposta, quando vemos que pode haver um ataque a um nome de domínio, especialmente nos dados de registro, o

endereço principalmente outros dados sobre o registrante, e observamos que são suspeitos, enviamos um e-mail ao endereço de e-mail fornecido no momento de registro, e fazemos cópia para o registrador, e antes de eliminar nomes de domínio, nós entramos em contato com um registrador, para garantir que ele tenha a oportunidade também de contatar o registrante. A maioria das vezes no passado, encontrávamos um pouco de resistência por partes dos registradores, não queriam divulgar as fontes, os dados que tinham, mas finalmente eles sempre têm nos ajudado, especialmente com esse plano de qualidade de dados.

BOBBY FLAIM: Agora vamos para Michele.

MICHELE NEYLON: Obrigado, sou registrador e provedor de hospedagem, gostaria de falar brevemente sobre alguns dos desafios que outros registradores e provedores de serviço encaram. Alguns dos desafios, nós como registradores, e como provedores de hospedagem, um dos grandes problemas é em relação aos relatórios, nos últimos anos, houve várias iniciativas em diferentes partes da comunidade anti abuso, para melhorar a qualidade dos relatórios. Na verdade, não foram até agora estabelecidos nenhum padrão, então não há uma padronização

das respostas também. Então as mensagens para vocês que querem nos enviar algum relatório, você nos dizer qual é o tipo de abuso, exemplos claros desse abuso, hoje quando eu fui no nosso escritório de relatórios de abuso, disse: o domínio X está envolvido num abuso, bom, isso não ajuda em nada. Eu preciso saber exatamente qual é o tipo de abuso, como ocorreu esse abuso, e também quando se fala de abuso, vendo em termos de não ampliar muito esse escopo, nós como provedores de hospedagem, não queremos que alguém nos peça para ser o juiz, o advogado e o carrasco. Nós precisamos ter claro o que, que aconteceu, o que, que você espera que a gente faça, no caso de malware, botnet, e em geral a gente não quer que esse tipo de conteúdo esteja nos nomes de domínios relacionados à nós. Mas nós como registradores, não temos nenhuma ferramenta de retirar partes do domínio. Eu posso deletar todo o domínio e serviços associados. E então eu gostaria que vocês entendam o que vocês têm que nos relatar, e o que, que nós podemos fazer e quais são os limites disso. Eu vejo que membros do CCTRT estão aqui, que estão fazendo uma revisão que inclui abuso, e talvez nos tragam dados concretos, dados que nos ajudam, dados que por exemplo, há uma relação entre nomes de domínios com certa extensão, com estratégias de preço por exemplo, mas dados reais são importantes, e não apenas teorias. Outra coisa é que nós como registradores, queremos trabalhar com o resto da comunidade, mas nós temos limitações do que nós podemos

fazer, então se nós pedimos mais detalhes, não é para complicar as coisas, mas queremos saber qual é a queixa, o que, que vocês estão reclamando. Eu não tenho muito mais para reclamar, mas da nossa perspectiva tem a ver com a qualidade dos informes dos relatórios. Eu acho que a comunidade poderia melhorar a forma com que relata os abusos para obtermos uma ação mais positiva.

BOBBY FLAIM: Michele, quando você falou de especificidade você poderia dar algum exemplo? Segurança operacional, uma empresa ou alguma parte, um grupo que permita que você atue?

MICHELE NEYLON: No caso de uma força policial, que apresentemos os logs, se você está agindo como registrador, você pode pedir que a gente deletou suspenda o DNS, depende do caso, mas a questão, ao invés de dizer para nós: há um problema, hás um problema tal e a gente quer que você faça isso, isso e isso. Por exemplo, algo bastante comum é a jurisdição, a minha empresa é irlandesa, você trabalha no sistema judicial Americano, então se você pedir que eu faça alguma cosia que tem a ver com a legislação Americana, eu digo: olha, sinto muito. Mas se você me mandar dizer, por exemplo, DMCA, eu como empresa da Irlanda eu não estou ligado ao DMCA, eu não posso atuar sobre o DMCA, mas

não significa que eu vou ignorar o relatório, mas eu não posso atuar diretamente em outras áreas. La Chapelle's está trabalhando em padrões de relatórios, por exemplo, a jurisdição, qual é a legislação, qual é a ação esperada, quanto mais específico for o relatório, mais fácil para nós é determinar se temos informações para tomar alguma medida, ou dizer: olha, excelente, mas a gente não está nessa jurisdição, ou precisamos de mais detalhes.

BOBBY FLAIM: Obrigado Michele, eu sei que essa é uma questão bastante sensível, porque não há um tratado internacional em relação do DNS, estamos falando em conflito de legislação, nós usamos MLAT que é um tratado mutuo, e eu sei que há desafios específicos, podia esperar um pouquinho as perguntas, só a Denise, ela é a última apresentadora, e depois a gente pode então responder as perguntas.

DENISE MICHEL: Eu gostaria de destacar os principais desafios dos usuários e clientes. Então muitas empresas têm adversários como Facebook, um único nome malicioso pode atacar várias plataformas muitas vezes isso é ignorado e um nome de domínio inteiramente qualificado é um nome completo, o nome do host, e nome de domínio, então com um único nome de

domínio malicioso em que há um espalhamento de muitos desses defeitos, e há várias consequências importantes como resultado de um único nome de domínio malicioso, e há uma série de slides que eu tenho aqui, eu vou publica-los na página da sessão, com uma referência de elementos importantes para, sobre com o RAA e o RA, tudo isso relacionado obrigações contratuais para ajudar a mitigar o abuso e também os registros e registradores que podem e devem agir para mitigar a função de obrigação disso. Então eu gostaria de destacar um exemplo da vida real. Por exemplo, dois nomes de domínio que foram registrados, um é .com, e outro .com-video.net e o login account.net, foram registrados usando nomes completes do Facebook, e detalhes de contato do Facebook, e como podemos ver aqui, toda essa informação que estava no Facebook, inclusive um endereço de e-mail, exceto os servidores de nomes. Então esses dois nomes de domínio foram utilizados para lançar malware de phishing, e outros ataques abusivos, e isso foi detectado pelo Facebook, e foi bloqueado, foi denunciado ao registrador, e isso passou também para a equipe de qualidade, o registrador não verificou o registro de nomes de domínio utilizando os endereços de e-mail que nós tínhamos, nós então apresentamos uma queixa tentando contatar o registrador várias vezes e apresentamos uma queixa, e perante o cumprimento da ICANN que foi aberta e foi encerrada dentro de 24 horas, e isso é feito, cancelamos os números de registro,

apesar de que o registrador tivesse reconhecido, registrado esses nomes. Então o sistema pode falhar, o que nós aprendemos dessa situação, o sistema falha se o registrador não presta atenção, se não toma ações apropriadas, segundo o RAA, e nessa instância, online NIC insistiu em obter a aprovação do titular da conta para modificar o WHOIS, é o mesmo tipo de conta do outro nome de domínio, então isso indica que o sistema falha, e então é preciso trabalhar de forma cooperativa com o registro que não o cumpre. E como plataforma global o Facebook entende bem que os procedimentos para defender-se de abusos não são perfeitos, e todas as partes às vezes falham na prevenção de ataques. E quando são identificados os problemas nos procedimentos e são melhorados ou modificados, essas situações podem melhorar. E muitas vezes temos essas falhas de procedimentos, e não devemos então aqui intentar a roda de novo. Já obrigações, já contratos e são utilizamos corretamente pela maioria dos registradores de registros, muitos estão aqui nessa mesa, e devemos implementá-los em todas as partes. Muito obrigada.

BOBBY FLAIM: Muito obrigado Denise, temos 12 minutos para perguntas, peço desculpas aqui, Peter você tinha uma pergunta pendente, então sinta-se a vontade para perguntar.

PETER VAN ROSTE: Obrigado Bobby, muito boa tarde para todos, eu sou Peter Van Roste, eu sou o presidente, o gerente geral do CENTR que é para os ccTLDs europeus, e eu quero responder uma coisa que disse Michele sobre a falta de compreensão dos diferentes fatores que aumentam ou diminuem os abusos nos nomes de domínios. Fizemos um estudo no nosso centro, eu vou compartilhar com você, e, além disso, sabemos que alguns membros do centro, fizeram estudos detalhados e exaustivos sobre vários atores específicos. Não sei se já foram publicadas as pesquisas, mas eu sei que eles têm intenção de divulgá-las, e segundo o que é crucial para a discussão, ou pelo menos para os europeus, é que a discussão, temos tido discussões para o Mercado único digital, e que também devemos seguir uma regulação de revisão da produção de consumidores. E a proposta então é ajudar a resolver, ou ajudara proteger os consumidores europeus encerrando os nomes de domínios, ou desabilitando temporariamente o acesso aos conteúdos. Não temos um texto em comum que expresse esses procedimentos. Então, eu sugiro ao painel de ver se há uma oportunidade dentro de toda comunidade, não apenas nos ccTLDs, para lidar com esse problema. Isso deverá ser tratado e resolvido daqui apouco.

BOBBY FLAIM: Alguém tem algum comentário sobre isso?

MICHELE NEYLON: Ajuda muito Peter, ter essas estatísticas de dados, o problema é claro, é que estava falando com gTLDs e não ccTLDs. Eu concordo100% que Cs e Gs são domínios. Muito obrigado.

MICHAEL PALAGE: Uma pergunta para o Allen, então a ICANN, a conformidade da ICANN ela recebe relatórios de abuso de terceiros como relatórios de SPAM etc., eu estou perguntando em geral, eu fiz uma solicitação recente, quais são as fontes que a ICANN está usando, e não ouvi resposta, então a ICANN não respondeu dizendo que era uma questão de confidencialidade, eu gostaria de saber quais são os recursos que as equipes de segurança da ICANN fornece para que a sua equipe faça o seu trabalho.

ALLEN GROGAN: Eu não posso falar disso com segurança, nós não utilizamos fontes de terceiros, a equipe de SSR utiliza essas fontes. Você está se referindo…

CARLOS ALVAREZ: Então quando alguém faz uma queixa, e não recebe uma resposta, pede para a ICANN responder…?

MIKE PALAGE: Eu acho que o grupo de CC, eles iam realizar uma análise do abuso das gTLDs tradicionais. Então há uma análise histórica em relação à situação atual. Onde são coletados esses dados para fazer isso, os dados precisam ser coletados.

CARLOS ALVAREZ: Eu acho então que pergunta certa seria perguntar para essa equipe para ver que recursos utilizam, vocês poderiam compartilhar? Então vocês estão operando em silos, a pergunta na verdade é comunicação, nós não publicamos relatórios de abuso. Essa não é a nossa tarefa. Nós analisamos dados de abuso, identificamos registradores, com domínios que podem ser considerandos maliciosos, mas isso é repassado dentro do processo para os registradores.

BOBBY FLAIM: Desculpe só temos alguns minutos.

KIRAN MALANCHARUVIL: Em primeiro lugar, foi uma excelente sessão, eu gostaria de saber a resposta do Grogan em relação ao Facebook, a fralde do registro do WHOIS é um problema muito importante, recentemente foram enviados dois relatórios à ICANN com

milhares de nomes de domínios registrados em .feedback cujos registros do WHOIS foram retirados que eram um site espelho, então eu gostaria de saber o que, que o Senhor Grogan tem a dizer sobre a preocupação da Denise quanto à como essas queixas são lidadas.

ALLEN GROGAN: Eu diria duas coisas, em geral nós não abordamos casos particulares em fóruns públicos, e também eu não revisei este ou outras queixas para essa sessão, então eu não posso abordar isso.

KIRAN MALANCHARUVIL: Então você nunca viu o WHOIS fraudulento antes?

ALLEN GROGAN: Essa não é essa pergunta, você me perguntou para abordar a questão específica que a Denise fez em relação ao Facebook, e eu não posso responder isso.

KIRAN MALANCHARUVIL: Agradeço ao painel, vocês estão falando por dois nomes de domínio fraudulentos, e que demorou quase dois meses para retirar esses domínios, em primeiro lugar eu gostaria de dizer que o ponto registro nós temos mais de 200 registros, e se chega

alguma queixa dos registradores, eles têm um tempo para tomar alguma medida, se isso não for feito, então haverá uma ação por parte, o registro deve tomar uma ação. Por que, que vocês não escrevem diretamente para o registro, e tem que esperar dois meses escrevendo para o registrador, para que ele entre em contato com o registro, e não fazem esse contato diretamente?

DENISE MICHEL: Nós fizemos o contato com o registrador diretamente, que foi responsável pelo registro do domínio para obter, fazer com que o registrador cumprisse a sua obrigação, e esse, para ter todas as informações desse domínio, e nós contratamos a conformidade da ICANN e pedimos que tomasse a medida que cumprisse com as obrigações sobre o RAA, esse é o processo e a obrigação contratual dos registradores, e nós precisamos seguir esses procedimentos, e as obrigações que são determinadas no contrato com a ICANN. Nós sabemos que os registros também têm responsabilidades, os registros que eu mostrei no meu slide, e isso é muito prevalente em alguns registradores, esse tipo de comportamento, então nós achamos que era importante que isso fosse relatado, o quanto tempo demorou para retirar esses domínios. Bom, mas eu discordo de certa forma, que você tem que passar pelo comitê de queixas da ICANN, se o

registrador não tomou nenhuma medida, você podia ter ido direto para o registro.

MICHELE NEYLON: Desculpe, eu acho que a Denise está reclamando dos nomes de domínios .com, e como tal o registro não tem os dados do WHOIS, então se reclamar para o registro, então se você vai reclamar para o registro, muitas vezes ele vai acabar reclamando para o registrador, mas o .com e o .net, são os registradores que tem o acesso aos dados do WHOIS, e não os registros. Por exemplo, se fosse .org ou outros TLDs, a relação é um pouco diferente, mas quando se fala .com e .net, os dados do WHOIS estão em posse apenas do registrador. Então o que eu estou falando é o seguinte, no caso do registrador não tomar nenhuma medida, o registro, eu acho que talvez a gente possa discutir isso fora. Nós ainda temos algumas perguntas para responder.

PAUL McGRADY: Por 15 anos, aconteceu comigo o que a Denise descreveu, e isso já aconteceu, e aconteceu isso com vários nomes de domínio que tinham as informações do cliente, as nossas, e nós então fizemos uma queixa, o registrador, não era baseado nos Estados Unidos, mas eu apenas suspendeu o nome de domínio, e não apagou, e a ICANN nos disse que depois que esse nome de

domínio é suspenso, ele não é jamais um nome de domínio é apenas uma política, então eu acho que é um problema isso, porque de repente você tem que suspender esse domínio todos os dias, então eu acho que essa prática não é boa, e isso era de um tempo anterior, mais feliz da internet. Eu acho que a ICANN deveria pensar melhor nisso e ver como isso pode ser feito de uma forma melhor. Em relação aos registros do WHOIS, e essas situações são bem diretas.

BOBBY FLAIM: Última pergunta.

NICK SHOREY: NickShorey do governo inglês, eu gostaria de dizer que foi uma discussão excelente, muito obrigado por organizar essa sessão, muitas ideias boas surgiram e podem ser desenvolvidas, colaboração como melhorar as solicitações de segurança pública, o que me parece dentro dessa discussão é definição quando se fala de abuso, o que, que a gente quer dizer com isso, e também há uma diferenciação entre pro ativo e reativo nas respostas ao abuso, em relação à validação do WHOIS, e nós temos as ações reativas, eu que sou um técnico, na verdade eu sou leigo, eu não sou técnico, então se há toda uma URL que é feita uma solicitação e se há um cyber crime, por exemplo, relacionado à ele, o que, que é feito? Eu acho que seria

excelente fazer, termos aqui também um operador de redes, uma empresa de hospedagem, eu sei que nós somos reguladores, mas eu gostaria muito de ter esse outro ponto de vista também. Eu acho que seria bom que alguém fizesse só hospedagem ou operação de redes, eu acho que contribuiria muito para esse debate, muito obrigado.

BOBBY FLAIM: Eu acho uma excelente ideia.

MICHELE NEYLON: Nick, eu sou registrador operador de redes e hospedagem, eu acho em termos sobre a query do DNS sobre as URLs, precisamos falar mais sobre isso. Então não se vê nenhuma solicitação no seu registro, se veem os outros níveis, mas não o WHOIS, então eu posso conversar com você sobre isso, obrigado.

CARLOS ALVAREZ: Carlos da ICANN, do SSR, eu só gostaria de acrescentar que há mais de dois mil registradores, e decidimos pesquisar poucos investigar, em geral malware, botnet e phishing, e isso tá dentro do mandato da ICANN. Há vários comentários da comunidade em relação à segurança, com relação a registradores, quando há o controle do SPAM pela ICANN isso não é do mandato da

ICANN, isso não está mencionado nos estatutos, a gente não pode pesquisar esses registradores, se quisermos revisar nossos registradores, tem a ver com o cumprimento do contrato. Então, o que eu gostaria de destacar aqui é que depende mais da comunidade abordar essa questão. Eu sei que a gente recebe as vaias, mas não somos nós responsáveis por isso. Muito obrigado.

ALLEN GROGAN: Rapidamente nós já passamos, eu quero falar da equipe do caso da Denise, só para deixar claro que os nomes de domínio foram suspensos ao primeiro contato, só isso que eu quero dizer.

BOBBY FLAIM: Giovanni tem um último comentário, depois Alice vai…

GIOVANNI SEPPIA: Muito obrigado Bobby, eu acho que a discussão dessa sessão tão curta destacou a importância da educação, cooperação e educação de todos os stakeholders, a questão de abuso não é apenas culpar alguém, mas é uma questão de se comunicar e saber o que nós podemos fazer juntos.

DENISE MICHEL: E bom, nesse espírito é importante saber que o WHOIS fraudulento, o nome de domínio usado para atacar os usuários da internet, e tem as informações da minha empresa, não deve permanecer suspenso no nome de domínio, eu não tenho dúvida que o Knightside foi o registrador. Essas duas teriam sido verificados pelo e-mail, e isso pode ter escapade em 24 horas, esses sites estariam totalmente suspensos, suspensão não é uma solução, nesse caso nós levantamos isso como um problema, isso não é a única vez, há vários desafios nessa área, eu quero destacar de que a conformidade está sendo uma prioridade do nosso CEO da ICANN.

ALICE MUNYUA: Muito obrigado, eu gostaria de primeiro agradecer aos painelistas pelas informações, e também por se manter no seu tempo, gostaria de agradecer a todos pelas excelentes perguntas, eu sei que vocês têm muito mais perguntas, e os painelistas tem apresentações mais detalhadas, e os que quiserem saber mais dos tópicos apresentados hoje, os Power Point vão estar online, agradecer a todos, nós temos a próxima sessão que é o WHOIS em 5 minutos, obrigada.