ABU DHABI – Sessão entre comunidades: Denúncias de abusos de DNS para desenvolvimento de políticas e solução de problemas
Segunda-feira, 30 de outubro de 2017 – 13h30 a 15h GST
ICANN60 | Abu Dhabi, Emirados Árabes Unidos

IRANGA KAHANGAMA: Boa tarde a todos, nós já vamos começar, peço que tomem seus assentos. Eu gostaria de agradecer a todos por vir aqui sobre denuncia de abuso para elaboração de políticas, sou Iranga Kahangama, um dos organizadores desse evento. Eu estou aqui como membro do FBI.

CATHRIN BAUER-BULST: Sou Cathrin Bauer-Bulst, uma das vice-presidentes do grupo de trabalho de segurança com o GAC e estou com a Comissão Europeia.

IRANGA KAHANGAMA: Então, vou dar uma visão geral do histórico ou dos antecedentes desse evento, e a Cathrin vai falar da logística desse evento, da perspectiva do grupo de trabalho de segurança da mitigação do abuso do DNS que queríamos estocar para a comunidade da ICANN, é um progresso natural de outras coisas que foram feitas a partir da recomendação do GAC sobre o abuso do DNS. Então,

ficamos muito interessados em fazer essa sessão intercomunitária e queríamos falar mais com a comunidade para ver como abordar essas questões. Eu vou falar brevemente do histórico, tivemos três teleconferências desse grupo de trabalho para determinar como faríamos esse evento. Nós pensamos então em trabalhar com princípios, havia diferentes perspectivas sobre essa questão, então decidimos discutir isso com a comunidade mais ampla. Então, esse evento foi bloqueado e nós vamos falar de três questões sobre a identificação do abuso, a denúncia do abuso e as estatísticas, como os dados devem ser usados. Então, eu gostaria de pedir a sua participação sobre esses três temas gerais.

CATHRIN BAUER-BULST: Então, eu gostaria de apresentar brevemente o que vamos fazer, temos duas apresentações curtas de David Conrad e Drew Bagley, e teremos um painel de representantes dos diferentes grupos participantes dos diferentes grupos que contribuíram para a preparação dessa reunião. Alan Woods, Graeme Bunton, Tania, Denise Michel, da parte comercial, Jonathan Matkowski, do IPC, Rod Rasmussen, presidente do SSAC atual, e Jamie Hedlund, das salvaguardas do consumidor da ICANN.

Como Iranga estava falando, estamos tentando estruturar essa discussão. Vamos então ter duas apresentações breves e tentar

discutir as três categorias que foram identificadas. Quando discutimos os princípios, não concordamos quais princípios seriam aplicados para a coleta de dados e o seu uso, os princípios aplicados a esse processo iam responder três perguntas-chave que vocês verão nesse slide e vamos voltar aí. Essas perguntas são como identificar o abuso do DNS de forma confiável, como criar uma denúncia eficiente e transparente, e como vamos usar esses dados. São essas três sessões que esperamos discutir com vocês hoje e embora tenhamos um painel muito grande de especialistas, é muito importante a sua participação.

Novamente, teremos essas duas curtas apresentações e vamos discutir cada uma dessas perguntas com os panelistas. Então, gostaríamos que vocês pensassem nas perguntas, em perguntas gerais ou específicas, por favor, não esqueçam de se identificar. Temos aqui funcionários da ICANN, levantem a mão e digam quando você quer intervir e vamos criar um espaço para isso. E para que todos possam participar, o tempo será de dois minutos para cada pessoa comentar. Então, gostaríamos muito que você compartilhasse, gostaríamos muito da sua participação e contribuição, o sistema de atividades de denúncia de abuso de DNS.

DAVID CONRAD: Eu sou David Conrad, nós desenvolvemos o que queremos, um sistema de denúncias de atividade de abuso de DNS. Bom, sou eu mesmo que tenho que mudar, gostaríamos de saber o que é esse sistema, ou DAAR, como nós chamamos, Domain Abuse Activity Report, é um sistema que permite a denúncia de registros de domínios e de abuso em registros e registradores. Por enquanto, está enfocado nos gTLDs porque são dados que podemos analisar mas não precisa se limitar a isso se os ccTLDS que quiserem participar, podemos discutir isso. O que é diferente de outros sistemas de relatoria? Há um grande número de mecanismos de relatoria ou de denúncia, a maior parte está associada com produtos comerciais. O que estamos fazendo é estudar todos os registros e registradores de gTLDs dos quais podemos coletar dados, estamos tentando usar um grande número de fontes de dados, e também verificar a sua reputação através de feed. Coletamos os dados por um período de tempo, para permitir estudos históricos, e tivemos que ver várias ameaças que foram identificadas no comunicado do GAC de Pequim, BOTNET command and control, spam foi incluído na nossa análise, o que foi meio controverso, como um vetor de outras formas de abuso.

E também fornece um índice ou informação para nós, porque em geral quando um TLD é atacado por um malware de uma

forma ou de outra, ou atividade maliciosa, também é afetado por spam. Então, um desses pontos importantes, tentamos ter uma perspectiva científica sendo mais transparente possível, que esse processo fosse repetível, então um distribuidor mostrou que um grande número, ou 100% estavam relacionados a spam ou a abuso, e o domínio de topo tinha uma cadeia de caracteres que esse revendedor de segurança estava olhando, era o .zip, e o zip, todos os domínios do .zip foram considerados maliciosos. Então, há uma série de questões que foram levantadas pela empresa para a ICANN e para a comunidade em geral, então várias pessoas, deve ser produzida uma lista, uma metodologia bem documentada que deve ser acordada para que não sejam utilizados, os relatórios serão utilizados para interesses comerciais.

Próximo slide. É uma questão de tecnologia, então o DAAR usa muitos conjuntos de dados, coletamos dados de abusos denunciados pela indústria e pelos internautas. O projeto deve ser repetível por qualquer um, então temos que usar dados publicamente disponíveis, não confidenciais, e correlacioná-los, gerando as planilhas que documentam as várias categorias. Os dados de abuso que estamos coletando são usados por sistemas de segurança comerciais que protegem milhões de internautas e e-mails. Estudos acadêmicos nesse setor validaram esses

conjuntos de dados, a estrutura que elaboramos é ter um marco ampliável e estamos fazendo experimentos, analisando diferentes subconjuntos de dados para entender melhor o que está acontecendo, a principal questão é que o DAAR, o ponto aqui é destacar que o DAAR é uma ferramenta que permite que a comunidade da ICANN veja como o ecossistema de nomes de domínio está sendo visto fora da comunidade. Surgiu uma pergunta sobre os critérios para selecionar os conjuntos de dados, e esse slide mostra os critérios que são usados na versão atual do DAAR.

Uma das atividades que estamos realizando foi solicitar ao RSSAC contribuições, o que deveria ser usado no DAAR e estamos agora desenvolvendo um NRFP, uma consultoria de especialistas independentes quanto a metodologia, e ao recebermos essas informações vamos escrever o documento descrevendo a metodologia proposta e isso vai ser colocado para comentário público e os fins de dados vão ser modificados de acordo com as contribuições. No momento, as exigências que a comunidades de segurança confie nesses dados, todos os conjuntos de dados precisam de ter um processo muito claro através do qual o nome é acrescentado ou retirado da lista de bloqueio. Então, essa classificação de ameaça deve refletir no que precisamos, então a .NET, destruição de malware e phishing

são os principais. Os RBL são adotados pela comunidades de operações de segurança e são feeds incorporados no sistema de segurança comerciais usado por operadores de redes, por exemplo, para proteger os servidores de e-mail, etc. Então, eu gostaria de esclarecer que quando essas listas de bloqueio de fama estão em todas as partes, nos browsers, nas nuvens e nos sistemas de conteúdo. Houve em Copenhagen uma apresentação de um grupo em relação à segurança, isso foi feito por Paul Vixie que desenvolveu um software que utiliza o chamado zona de políticas de resposta que permite bloquear nomes de domínio.

Sabemos que alguns provedores de internet e e-mail bloqueiam TLDs inteiros porque acham que estão cheios de malware. Além disso, os operadores de redes privadas usam os RBLs e os firewalls comerciais, essa é uma lista o que estamos usando, desculpe passar um pouco do tempo no sistema DAAR, temos basicamente sete RBLs e uma delas é uma lista composta que tem várias outras incluídas. Então, por que o DAAR tem essa denúncia de domínios de spam? Na verdade, o spam são os domínios que mais ameaçam a segurança, então o sistema DAAR mede os domínios que estão dentro do spam e não nos spams em si, então passo a palavra a Drew Bagley.

DREW BAGLEY: Obrigado. Sou Drew Bagley da fundação de segurança de nomes e domínio, e com base na apresentação do Dave sobre o valor desses dados e a confiabilidade, eu quero falar como usar esses dados para bloquear TLDs, ao invés de informar a política que pode ajudar a melhorar os esforços para manter uma internet aberta e livre, e não rodar essa ideia contrária da aceitação universal. Há consenso na comunidade sobre formas de abuso, especialmente phishing e malware, que estão proibidos pelos acordos e também quanto aos mecanismos mais comuns de envio através do spam.

O que é importante é que a comunidade entenda quando trabalha com a questão dos abusos é não ficar presos nas diferentes interpretações do que o abuso que nos proíbem fazer qualquer coisa a respeito do abuso. É muito importante que a comunidade comece a trabalhar sobre as questões de política quando houver consenso e também utilizar métricas confiáveis para o phishing, malware e spam e também para o controle do botnet. Como parte da equipe de revisão de ACCT, nós temos observado o problema dos abusos de DNS relacionados com salvaguardas implementadas para evitar abusos nos gTLDs. Para medir isso, há um proxy que estamos observando, quando observamos malware, spam ou phishing e encomendamos

pesquisa de dados similares aos apresentados pelo Dave para fazer recomendações e normativas.

Esse é um exemplo de como utilizar os dados para poder fazer políticas orientadas aos dados. Descobrimos depois de análise que o abuso é algo inteiramente não universal, nem aleatório. Conseguimos certificar fatores que tinham mais probabilidade de estar em relação ao aumento do abuso em zonas ou registradores particulares, ou com baixos níveis de abuso, operadores de registro determinados. Houve restrições, cada vez mais restrições no registro com menores casos de abuso, e os operadores de registros tinham a tendência de ter maiores correlações com abusos de maior nível e ao mesmo tempo com preços baixos.

E também, fazendo uma análise bem micro, descobrimos que havia uma correlação forte entre os termos de marca registrada em campanhas de phishing, isso não é de surpreender, houve um exemplo bem específico que envolvia seis nomes de domínio que permitiam permutações diferentes de marcas registradas da Apple como iPhone e outros através de campanhas de phishing. E também 76 nomes de domínio, e acho que também 83 instancias de abuso desse TLD. O que os dados notaram é que aqui há uma brecha nas normativas, e o que a comunidade está fazendo para analisar esses conjuntos grandes de dados,

especialmente dependendo do WHOIS para poder determinar mecanismos mas ao mesmo tempo isso não nos resolve cada um dos problemas para detectar os mecanismos subjacentes que afetam a estabilidade do DNS. Vou destacar dois registradores que são especialmente problemáticos com os conjuntos de ferramentas existentes.

O primeiro é um registrador que foi suspenso mas conseguiu operar para a maioria de todos os abusos de alto nível de 2016, e ele finalmente pagaram as contas mas se você tem que fazer delitos cibernéticos, tem que pagar as contas, o que aconteceu é que nesse modelo de queixas tivemos uma abordagem reativa dos abusos e decidimos agir com essas queixas na comunidade e ao mesmo tempo utilizando esses conjuntos de dados do DNS como é o DAAR, para detectar problemas de forma proativa e agir ao invés de esperar a uma reclamação ou infração de vitima afetada pelas ações maliciosas.

Aqui está o segundo registrador com os nomes envolvidos, ainda está operando, a UPnames, e foi feita também uma pesquisa de ccTLDs, se esse registrador oferecia registros a granel pelos quais um registrante poderia recorrer à UPnames e registrar 2 mil nomes de domínio de uma vez só, e a UpNames poderia gerar consequentemente esses nomes para os usuários. Você tinha então seus nomes registrados e esse registrador

tinha altos níveis de abuso mas sem que houvessem queixas, e sem um procedimento de suspensão subsequente. Essa também aqui, isso representa também uma brecha potencial nas políticas para tratar essas questões.

E também aqui a revisão de ccTLD utilizou esses dados e elaborou políticas de recomendações para a comunidade e estarão disponíveis na semana que vem e nossa equipe com todos esses dados temos trabalhado de uma maneira transparente através do DAAR e também da comunidade de cyber security, como comunidade devemos bloquear mas também identificar brechas, criar políticas ou incorporar dados para novas políticas. Através disso, os operadores e registradores ficariam em risco e para eles seria mais difícil repetir suas violações. Eu espero que esse painel possa discutir isso de diferentes perspectivas, algo que a comunidade precisa muito, precisamos de dados que sejam funcionais e que possam ser utilizados para criar políticas para termos um DNS que seja melhor para todos nós. Muito obrigado.

IRANGA KAHANGAMA: Temos dois minutos a mais, começarei com a sessão de perguntas entre os membros do painel, sintam-se à vontade para responder, e também o público para participar. Alan, não

sei se você se importa de começar com a parte superior da cadeia.

Quando temos um abusador muito evidente, que ações e que ferramentas deveríamos utilizar ou o registro deveria utilizar para transformar as tendências observadas de abusadores repetitivos e identificar os problemas.

ALAN WOODS: Você falou sobre abusadores óbvios, mas infelizmente vemos os dados que vem das fontes tão fantásticas e uteis, mas realmente não poderíamos falar em abusadores óbvios ou evidentes, podemos agir ou encaminhar essa questão a um registrador, então a primeira pergunta é, como sabemos que um abusador é óbvio? Quando temos informações ou provas, utilizamos, revisamos, analisamos e encaminhamos à parte pertinente, e se o registrador não age ou o registro não age, deveríamos encaminhar para outra instância. Sim, observamos os indicadores recebidos, por exemplo, as listas como a Spamhaus ou a SURBL, mas precisamos de mais informações e mais provas.

IRANGA KAHANGAMA: Obrigado, as estatísticas são boas sim, mas precisamos continuar pesquisando.

ALAN WOODS: Eu sei que essa é uma questão controversa, essa é uma orientação, mas as únicas provas que encontramos são os nomes nas listas negras, precisamos de mais detalhes e maneiras suplementares para determinar uma razão de por que estão na lista, apenas uma manifestação vazia, o que faz com que seja muito difícil identificar as razões, por exemplo, por trás de um flashpoint, é muito difícil obter informações especialmente das listas de bloqueio dos provedores, porque é um segredo industrial.

CATHRIN BAUER-BULST: David, você quer comentar algo?

DAVID CONRAD: Sim, quero adicionar alguns dos motivos do por que o DAAR inclui informações históricas para identificar tendências ao longo de longos períodos, incluindo o tipo de informação abusiva durante um longo período. Eu concordo 100% de que o conceito do óbvio é muito difícil de determinar, precisamos de mais informações para identificar os verdadeiros abusadores, e isso deve ser facilitado à comunidade, a comunidade deve fornecer informações para termos discussões sobre as normas que nos permitam identificar claramente as tendências de

abuso dentro de espaços de nomes determinados, muito obrigado.

IRANGA KAHANGAMA: Agora temos Rod.

ROD RASMUSSEN: Eu falo a título pessoal, não represento o SSAC, e eu vou responder diretamente essa pergunta. Ouvimos essa resposta sobre como é que uma organização particular identifica o abuso de forma segura, para isso precisaríamos de políticas confiáveis, e esse setor tem existido por 15 anos, com métodos confiáveis para identificar abusos, por exemplo, de forma sistêmica, também através do uso do internet explorer, do browser, do seguro da google que são colocados automaticamente de forma automatizada com segundos apenas para identificar, então o aspecto tecnológico nesse sentido é muito seguro, temos utilizado listas para reduzir os falsos positivos, até o zero, então há tecnologia disponível, mas importante levar essa informação para o campo da ação, e temos o criar um marco para agir em vários pontos no registro de domínio, provedores de e-mails, e isso está resolvido do ponto de vista tecnológico, mas não do normativo ou de políticas.

IRANGA KAHANGAMA: Alguém do público?

DAVE PISCITELLO: Dave, da ICANN. Não gosto desses termos de abusador óbvio. Não é o que mensuramos com a DAAR, mencionamos as ameaças à segurança, listas de bloqueio, listas de reputação, que são coisas diferentes do que a obrigação de um registrador ou companhia de hosting de DNS devem fazer, porque fazer uma pesquisa para corroborar uma reclamação. Eu, por exemplo, se estivesse nessa posição, tentaria chegar ao e-mail, URL, ir até o site, e há muitos procedimentos que especialmente quando estamos esperando a duo diligência, mas o DAAR não está concebido como o espaço para termos as respostas certas, mas devemos ter um certo sentido de toda a passagem dos abusos e ameaças e tentar ter alguns números que nos ajudem a identificar quando a política é bem-sucedida ou não.

CATHRIN BAUER-BULST: Obrigada, Dave. Quanto a questão dos registradores. Nós ainda não falamos sobre essa faixa de diferentes indicadores à disposição, temos o DAAR que fornece uma base para avaliação, e também sabemos que há mais necessidades para trabalhar do lado dos registradores com as informações e transformar em ferramentas funcionais e operáveis para agir contra possíveis

clientes que não cumprem com nossos termos e condições. Você poderia falar um pouco sobre isso?

GRAEME BUNTON: Eu acho que duas coisas interessantes, Alan levantou um ponto interessante, que ligar a lista de bloqueio com a comprovação não é trivial. O que o Dave disse é que os métodos que se pode usar para combater abuso na sua plataforma pressupõem uma sofisticação no monitoramento de abuso. Então, para reduzir o abuso, às vezes não se tem muito tempo para fazer. Eu vi nos domínios gerados por algoritmo, para gestão de nomes de domínio mas isso não é muito comum. Mas, é muito difícil de rastrear maus atores ou contumazes, não é simples de fazer e isso vai reduzir o abuso na nossa plataforma, mas demanda uma visão muito ampla do que entra nessas listas de abuso. Eu acho que Alan quer falar.

ALAN WOODS: Eu gostaria de dizer o que o Dave disse, se tivesse mais perto, eu acho importante o que o DAAR está fazendo, um projeto que mostra estatísticas, o que precisa ser feito entre o DAAR, o trabalho que o registrador e o registro precisam fazer. Você poderia falar mais especificamente que tipos de dados são necessários para permitir esse tipo de ação?

ROD RASMUSSEN: Há muitas metodologias, coisas que são fáceis de detectar, ou que são geradas por algoritmos nos nomes de domínio, por exemplo, um algoritmo de geração de nomes de domínio que é usado para malware, cria uma série de nomes que podem ser registrados no futuro. Então, outra coisa, isso é uma forma, spam é uma forma óbvia, isso tem sido feito há uns 10 anos, mas é uma análise rudimentar. Há várias plataformas, como Facebook, redes sociais, que usam esse tipo de análise. O programa de e-mail e plataforma de e-mails buscando conteúdo permitidos pelos usuários para ver o que está sendo feito. Com essas informações, podemos correlacionar com metadados, com consultas do DNS ou WHOIS e correlacionar com a própria base de dados, com objetos desconhecidos ou conhecido, e há ferramentas que podem ser adicionadas aos browsers, algoritmos bastante sofisticados para verificar a formação de tunnelling, e há muitas tecnologias que podem ser reunidas para fazer uma lista dessas diferentes áreas de abuso. Obrigado.

IRANGA KAHANGAMA: Uma coisa que ficou claro é que ter dados disponíveis é essencial. Então, nós vamos responder uma pergunta feita de forma remota.

CATHRIN BAUER-BULST: Eu gostaria de voltar aos diferentes tipos de dados que precisamos informar para elaboração de políticas. Drew falou sobre essas ideias de identificar as tendências gerais e precisamos de informações específicas para tomar medidas individuais que não depende, isso não cabe a investigação criminal. Eu gostaria que a Denise falasse de sua experiência específica para estabelecer padrões para a comunidade e clientes. Quais são as lições a serem aprendidas, quais as condições podem ser demandadas para permitir uma reação eficiente contra o abuso?

DENISE MICHEl: Bem, temos um enorme sistema global para segurança e mitigação de abusos em todas as plataformas que são continuamente monitorados e atualizados. Eu acho que é uma coisa muito importante que todos compartilhem as melhores práticas não só em termos de serviço mas também de compartilhar dados para aumentar a segurança, eu acho que também seria importante comparar o que fazemos e o que os registros e registradores fazem. Uma das questões que não foram abordadas são incentivos e a vontade de disponibilidade de fazê-lo. Quanto aos comentários, há o estudo de, então, o setor comercial fez vários comentários para esse estudo de

abuso, recomendações, ou por exemplo, ligar incentivos às melhores práticas, ver as taxas que os registros e registradores tem que pagar, ligar isso às melhores práticas, garantir, bom, isso é o primeiro estudo de abuso mas deve ser feito continuamente e termos dados de tendências que sejam rigorosos e aumentar a fiscalização da conformidade de registros com altas taxas de abusos. Quanto mais cedo começarmos, quanto mais cedo conseguirmos ver o relatório do DAR na forma beta, melhor, e quanto mais cedo conseguirmos dado, melhor.

Vamos passar a palavra para a plateia.

REG LEVY: Levy, de Tucows. Eu gostaria de abordar algo que alguém falou de termos e condições. É muito verdade que temos termos e condições que podemos tirar um site do ar por qualquer razão, que são para proteger, nos proteger e não para policiar a internet. Então, no momento em que houver algo que não decidimos antes e seja necessário, temos o direito legal de fazer isso, a gente não faz isso porque a gente quer, eu gostaria de fazer uma última pergunta para o Jonathan sobre uma coisa que apareceu na apresentação, a ideia de indicadores, Drew disse que há tipos específicos de abuso e vários veículos, um deles sendo spam. Às vezes infrações de direito intelectual

podem ser associadas com abuso ou ser indicadores de possível abuso. Você poderia falar de indicadores e sua utilidade para identificar abuso?

JONATHAN MATKOWSKI: Jonathan Matkowski falando a título pessoal. Em primeiro lugar, em termos de registradores, as obrigações no contrato de credenciamento, uma das coisas é responder ao abuso adequadamente, investigar. Isso é para benefício da comunidade, gostaria de instigar a todos a fazer isso, e garantir que a comunidade seja protegida de abuso. Sabemos que phishing está relacionado ao conteúdo, ele está relacionado ao roubo de informações pessoais e isso de muitas formas, o IP e o conteúdo estão relacionados, ameaças à segurança, especialmente ameaças complexas em que a localização de mais de uma, onde são localizados em mais de um lugar, faz um pop-up do Adobe, fazendo com que as pessoas façam download de malware. Os operadores de registro nem sempre tem visibilidade com os registradores que não respondem às queixas de abuso. Precisam ser notificados quando o registrador não for, quando esse registrador não estiver cumprindo com as obrigações, e essas informações estariam incluídas na estatística. Esse projeto DAAR deve ser usado internamente na ICANN para auditoria ad hoc.

E outro relatório, no SADAG, vemos que há menos denúncias de falta de cumprimento que falam sobre o volume de queixas de abuso e etc., o Dynamic Dolphins tem informações sobre isso. Obrigado.

IRANGA KAHANGAMA: Eu gostaria de passar para o próximo slide. Como criar denúncias de abuso eficientes e transparente, então há diferentes situações em que essa lista de bloqueios foram usadas, por diferentes browsers e provedores de e-mail. A minha pergunta é que os interesses dos usuários finais podem se sobrepor a algumas das análises estatísticas e dados de abuso do DNS podem ser usados para criar uma ferramenta amigável para informar o público dos riscos e abusos. Eu acho que não representamos os usuários finais, representamos os não-comerciais porque os finais podem ser comerciais ou não. O que eu gostaria de dizer é que temos uma posição em relação as ferramentas e sistema de denúncia de abuso. Estamos coletando estatística, não estamos retirando do ar o site, e qual é a ferramenta que posso usar? Eu estou a favor de compartilhar os dados, de coletar estatísticas, mas na ICANN temos que fazer uma linha muito clara entre o que é abuso de DNS e o que é relacionado a conteúdo.

Nem sempre o que é ilegal sobre a legislação em vigor é um abuso técnico. Ao que se pode, alguém fazer um RA, esse RA de 2013, que foi a missão da ICANN do período de transição. Eu acho que também falamos muito sobre essa abordagem preventiva, o que significa prevenir? Quais são os players que devem agir? Isso deve ser muito claro, eu acho que temos que ter uma definição bastante estrita de abuso do DNS, quanto aos usuários não comerciais, não devemos esquecer que a principal coisa não é tirar o site do ar, mas prender os que violam a lei. Não queremos uma polícia de conteúdo, por isso ficamos assustados quando escutamos falar que a indústria deve se policiar.

Eu acho que devemos lidar com o abuso de DNS, e não ser polícia de conteúdo.

CATHRIN BAUER-BULST: Vou passar para Drew, você do ponto de vista de pesquisadores em segurança, qual é a frequência com que esses dados devem ser publicados? Há uma frequência mínima, ideal para que seja útil para a comunidade de segurança?

DREW BAGLEY: Bom, se olharmos o estudo que foi encomendado pela comissão do CCT, então não é algo que aparece a cada 5 anos ou cada vez

que uma equipe de revisão aborda essa questão. Eu acho que como o DAAR produz estatística transparente para a comunidade, se isso fosse continuo seria excelente, e com isso poderemos fazer analises periódicas desses dados.

Então, podem haver análises mais específicas ou mais amplas como a comissão do CCT fez, talvez bianual, eu acho importante ter essa visão de longo prazo. Então, pode haver campanhas de softwares maliciosos, podem não aparecer em alguns trimestres específicos, é muito importante ter essa avaliação continua, a Tania fez um comentário excelente, eu acho que devem refletir a diversidade da comunidade e dos diversos pontos de vista. Passando anos debatendo diferentes coisas que poderiam ser abuso em um país e não em outro, eu acho muito importante, como comunidade, começarmos a lidar com coisas que são consenso. Ao invés de nos perdermos no caminho com conteúdo. A Tania mencionou isso, também acho que Alan falou muito bem sobre a dificuldade do lado de reação, de tentar encontrar os que cometem abusos. Como a Tania disse, um provedor não é uma força da lei. É por isso que acho muito importante passar para um modelo proativo para usarmos indicadores óbvios, então temos parâmetros para tirar um site do ar especialmente se o tiramos imediatamente ou esperamos para ver o que acontece.

Os planos atuais quanto a publicação dos dados gerados no sistema DAAR, a ideia é gerar um relatório mensal, essas estatísticas seriam agregando dados por registros e registradores, e isso estaria disponível através da iniciativa de dados abertos. Então, com o tempo as pessoas possam fazer análises de tendências históricas, com base nesses dados. Isso seria uma tentativa e gostaríamos muito de que vocês dessem suas contribuições sobre a frequência de publicação dos dados, quando será o primeiro relatório? Estamos fazendo uma avaliação das exigências de licença que temos com os diferentes feeds de dados. Então, eu não posso dar uma data aqui precisa, por causa dos advogados.

IRANGA KAHANGAMA: Então, passo para a plateia.

MILTON MUELLER: Sou Milton Muller da universidade Georgia Tech. Parecem haver duas abordagens diferentes quando se fala do DAAR, o David falou de coletar muitos dados, publicar relatórios, e esses relatórios para elaborar políticas, mas os registros e registradores disseram também que precisam intervir e falei de ações mais preventivas, então o que vai ser o DAAR? Por quanto tempo ele vai funcionar? As ameaças mudam, você está

dependendo em RBLs de terceiros, as ameaças mudam, as técnicas e os criminosos mudam. Como você vai responder a essas inovações? Vão tentar então desenvolver essa capacidade ou vão depender só das entidades de terceiros?

DAVID CONRAD: A resposta simples é fazermos o que a comunidade nos diz para fazer. Se no contexto do DAAR as ameaças identificadas são as do comunicado de Pequim e em algum momento a comunidade sugerir que devemos rastrear outras formas de abuso, podemos ver o que fazer, e isso se estende por mais tempo. Com relação às fontes de dado, são as publicamente disponíveis, se houver uma fonte de dados que a ICANN gerar, que pode se tornar disponível, podemos incorporar no sistema do DAAR. Depende da demanda da comunidade, meu coleta, Piscitello pode falar mais sobre isso.

DAVE PISCITELLO: Sim, fico contente por você ter feito essa pergunta, coisas que podemos fazer daqui um ano que não podemos fazer agora, temos um ano e meio de história. Migrar ou estudar o comportamento da migração, se há um pico repentino de registros para registradores e como são utilizados os nomes. Posso mostrar um gráfico, tem picos também para um

registrador determinado que tem um milhar de registros, são algumas das medições que são feitas pelo SADAG com base nas suas análises de compromisso dos domínios registrados.

Tenho tido conversas no sentido de fazer ou inicializar, adicionar a inicialização ou listas negras. Listas distribuídas para denegação de serviços em sites, que são uma ameaça que está crescendo e então devemos pensar em como vamos resolver isso em benefício da comunidade. Criamos uma plataforma muito extensa e muitas dimensões, devemos pensar como utilizar as medições. Eu estou pensando muito no que você sugeriu.

JAMES COLE: Obrigado. Acho que há perguntas remotas, podemos ouvi-las e depois vamos passar para a terceira parte da discussão. Temos a pergunta de Maxim Alzoba.”O escritório da ICANN está planejando, que recurso poderia ser utilizado para registros e registradores e qual o motivo para utilizar uma companhia com práticas questionáveis, Spamhaus, como prática confiável de bloquear a internet de registradores e do sistema sem responsabilização e transparência à comunidade”?

DAVID CONRAD: Vou responder à utilização do Spamhaus, acontece porque dentro da comunidade com abusos, Spamhaus é considerado uma fonte confiável, que cumpre com todos os critérios, temos feito uma construção, uma seleção para bloquear essas listas e isso independente dos e-mails, é o que achamos sobre uma lista de bloqueio, e que é a realidade, de como essa lista é utilizada pelos setores acadêmicos e indústrias para repercutir no tráfego da internet sempre assumindo que uma lista de bloqueio não é importante porque não aceita as políticas, não muda os fatos de que há outros que dependem dessa lista de bloqueio para bloquear o tráfego de domínios delituosos e os critérios mudam de maneira que o Spamhaus não seja considerado alternativa viável, então podemos ajustar as coisas conforme preciso e haverá evidencia demonstrável de que estamos em todas as especificações.

Nossa experiência foi que em muitos casos, o pessoal que reclama sobre bloqueios determinados é porque foram colocados nessas listas de bloqueio por algum motivo, e isso pode servir como motivo para que consideremos novamente incluí-los nos dados. Quanto a fornecer os dados à comunidade, como mencionado no nosso plano, nosso plano é disponibilizar os dados a partir da iniciativa open data. Atualmente isso está

no nosso plano para fazer mensalmente mas depende das necessidades e solicitações da comunidade.

IRANGA KAHANGAMA: Obrigado, David. Acho que há mais uma pergunta remota.

JAMES COLE: Essa pergunta vem de Kristina Rosette. “Quais mecanismos pensa a ICANN em implementar, disponibilizando publicamente os dados do DAAR?

DAVID CONRAD: Como mencionei, estamos gerando esses dados mas dependemos de terceiros, qualquer um pode assinar, pagar uma licença e se uma denúncia for um falso positivo, isso vai ter impacto em como esses milhões de usuários, os RBLs vão interagir com o recurso, um endereço IP ou nome de domínio. É verdade que houve falsos positivos, descrições frequentes de casos famosos de falsos positivos mas a realidade é que nós observamos, selecionamos uma lista de bloqueio e os critérios que utilizamos são por permissão da indústria e da academia, que eles tem processos documentados pelos quais os nomes são adicionados ou eliminados. Tem um mecanismo claro pelo

qual eles operam as listas de bloqueio, e quanto a questões de responsabilidade, não sou advogado, não posso responder isso.

CATHRIN BAUER-BULST: Obrigada, vamos à terceira parte da discussão, ver esses slides por alguns minutos e ver como podemos utilizar isso para fazer políticas e também pelas forças policiais. Não falamos muito sobre como isso pode ser usado internamente na ICANN. Vou perguntar ao Jamie. Você também tem necessidades nesse processo, deve ter pensado nisso para o futuro.

JAMIE HEDLUND: Queria mencionar que temos trabalhado estreitamente com a Octo num departamento contratual e estamos muito contentes com o DAAR por uma série de motivos, são evidencias baseadas nos dados e se for verdade de que essas listas da DAAR são feitas por companhias, empresas para tomar decisões quanto a serviços de e-mail, ou acesso à web, então isso vai facilitar o nosso trabalho, porque há registros que podem estar bem nos níveis superiores de hierarquia. Mas, os resultados do DAAR são os que o Dave explicou, e é que o nível acumulativo não é algo que possamos utilizar no departamento de cumprimento contratual. Isso para limpar alguns dos registradores e suas zonas, e por último, os resultados que eu vi mostram que há um

conjunto bem pequeno de partes contratadas que são responsáveis por uma grande maioria de níveis de abuso. Eu, frequentemente, não são instituições ou entidades, nunca foram participantes da ICANN pelo que eu tenho observado, e em geral também seria bom para credibilidade e legitimidade da ICANN de seu modelo multisetorial depois da transição da IANA, o que é muito importante.

ALAN WOODS: Eu gostaria rapidamente de agradecer ao Jamie, é bom ouvir isso. Também quero destacar que esse é um ponto muito interessante, temos esses atores maliciosos, eles existem, há muitos registros realmente tentando fazer o melhor possível e trabalhar de forma positiva, e nós da Donuts aplicamos a lei e podemos decidir e estamos muito contentes de poder contar com esses testes e evidências.

GRAEME BUNTON: Os registradores realmente querem jogar fora os maliciosos, os caras atores maliciosos, muito bom para todos nós, que estamos trabalhando para manter as plataformas limpas, reduz muito as consequências para as políticas ou soluções, deveriam estar bem focalizadas e acho que devem estar bem focadas nos atores específicos. Isso resolveria muitos problemas.

GREG MOUNIER: Greg Mounier da Europol. Uma pergunta para Graeme e Alan. A indústria de nomes e domínio é uma indústria bem direcionada, o que poderíamos fazer para tomar medidas proativas e quando é que vamos ver numa estratégia de marketing, como a Tucows, para dizer que a Tucows tem a menor taxa de abuso para podermos escolher, então?

GRAEME BUNTON: Muito obrigado, sim, Tucows é diferente, mas sim, isso introduz algum grau de responsabilidade e devemos observar os resultados gerais, ser proativos quanto aos registros, ainda essa situação não existe, não.

ALAN WOODS: Sim, com a Donuts também consideramos isso seriamente, também a iniciativa de nomes e domínio saudáveis de algum presidente, e isso faz com que sejamos bons atores e cada vez que eliminamos um domínio, isso faz com que o abusador deva ir para outra parte, então podemos eliminá-los da nossa plataforma, mas ele irá a outra plataforma.

ROD RASMUSSEN: Esse primeiro item de discussão, primeira reunião da ICANN, eu representava um setor de abusos e trabalhava com registradores e infelizmente isso foi em Vancouver, uma reunião e não consegui participar da reunião principal, isso é história, mas muito foi feito nos últimos 10 anos, com muito sucesso, e por exemplo o grupo anti-phishing, eu e Greg Aaron produzimos relatórios frequentemente desde 2007 sobre tendências nos registros e domínios utilizados para phishing, e esses relatórios foram utilizados juntamente com registradores e registros para descobrir tendências e problemas e mudar as políticas para lidar com eles. Isso no espaço da ICANN e dos ccTLDs, especialmente nesse último que tem tido problemas mais graves que limpamos, então enquanto os marcos para atacar isso, temos os contratos e então essas entidades devem trabalhar sobre a questão dos contratos e retirar os contratos ou também outra possibilidade de ter um programa de intervenção confiável para criar uma certa autonomia, automatizar essas condutas ou procedimentos, muito obrigado.

DAVID TAYLOR: Sou David Taylor, advogado, estou na equipe da ccTLD, de revisão, então estou com aquele cara de barba. Quanto a pergunta que tinha a ver com o apoio, as denúncias de abusos, essa é uma questão chave, há muitos registradores bons, ruins,

muito bons registros, outros não, devemos buscar, e buscar leva muito tempo, pode levar várias semanas, detectar e depois retirar um nome de domínio, mas quando chegamos a um registrador, em que James já mencionou isso, esse nível de abuso tão alto como o que percebemos do .SCIENCE, com alto nível de abuso, de 51%, na zona de nomes de domínio abusiva, vemos que isso leva tempo, de um ano, talvez seis meses, e por que demora tanto, quando parece tão óbvio? Mas eu acabo de entender por que é tão difícil, não posso explicar para os outros.

JAMIE HEDLUND: Há duas explicações aqui, uma é a evidência funcional contra os níveis de abuso não basta, precisamos de outras evidências, e em segundo lugar, há limitações no contrato e não podemos ordenar que um domínio seja eliminado ou retirado, e uma coisa que vai surgir, espero, é utilizar os nomes subjacentes, e nesse sentido podemos falhar ou não, mas nossos esforços por utilizar essas ferramentas feitas por nós, nos ajudam a informar à comunidade sobre a necessidade de elaborar uma política determinada, e a comunidade, pessoas como vocês, se formos bem-sucedidos, terão evidencia suficiente de que não está dando certo e isso será uma fonte de informações que nos ajudará a alterar políticas ou contratos. Último comentário do Iranga.

IRANGA KAHANGAMA: Obrigado, Jamie, muito rapidamente um último comentário antes de encerrar, e depois a Denise vai fazer uns comentários sobre a tomada de decisões.

DENISE MICHEL: Sim, temos o relatório de abusos, SADAG, que os novos gTLDs tem uma taxa maior de abuso do que os tradicionais. Temos esses dados que foram fornecidos nesse relatório, são muito úteis e pertinentes. Temos agora um PDP de proteção de direitos, e agora em andamento, que para criar políticas para a próxima rodada de novos gTLDs, é apenas um exemplo mas há muitos outros aplicados à implementação de privacidade ou proxy, e também iniciativas da ICANN mas quando se trata de contar com dados de abuso e informações e tendências, devemos informar toda essa atividade dentro da ICANN porque somos uma comunidade que usa dados e fatos reais para entender e que são a base da elaboração de políticas, isso que os advogados devem entender, podem utilizar o relatório DAAR na esfera pública, a iniciativa ODI, que seriam muito uteis.

DAVID CONRAD: Só para esclarecer um pouco, estava brincando quando falava sobre uma ação de bloqueio de advogados, devemos eliminar

alguns acordos de licença, demora um pouco mas vamos poder avançar e publicar relatórios e estatísticas num futuro próximo.

CATHRIN BAUER-BULST: Muito obrigada, está acabando o tempo, não podemos tomar mais perguntas, sinto muito e podemos, é um assunto muito interessante que exige continuar conversando e também perspectivas comuns com mitigação de abusos, há várias partes da comunidade que destacam a necessidade de elaborar políticas para tomar ações individuais e como um aspecto preventivo, inclusive reativo. Isso tem ajudado.

Isso é muito bom, porque focamos em ações especificas, temos 76 exemplos citados pelo Drew e isso seria outro campo grande de dados, para a agenda. Poderíamos voltar à ideia dos princípios que Iranga mencionou antes e continuar nessa linha.

IRANGA KAHANGAMA: Muito obrigado aos participantes, podemos continuar com essa conversa e agradecemos também que esse grupo de trabalho continue tendo essa discussão que merece realmente ter um nível das diferentes comunidades para fornecer mecanismos para continuar tentando resolver as questões de abuso do DNS. Vamos manter a comunidade informada de uma forma transparente para continuarmos avançando nesse sentido.

Obrigado então pela participação, continuem participando de eventos como esse.