
COPENHAGUE – Reunião pública do SSAC
Quarta-feira, 15 de março de 2017 – 15h15 às 16h15 CET
ICANN58 | Copenhague, Dinamarca

PATRIK FÄLTSTRÖM: SSAC reunião pública, dia 15 de março de 2007, às 15h15min. Eu pediria que os membros do SSAC viessem à mesa. Bem-vindo a todos, passou um pouquinho das 13h15min, então não é 08h00min da manhã da quinta-feira, embora a gente tenha tomado café aqui de manhã mudou a reunião, eu sou Patrik Fältström presidente do Comitê de Segurança e Estabilidade. Em geral nós nos encontramos às 08h00min da manhã para o café da manhã em uma sala muito menor do que essa, muito mais aconchegante, um dos deveres dos membros do SSAC é participar das sessões e nem todos podem estar aqui na mesa, mas eu pensei em apresentar à esquerda, então vão se apresentar.

ROD RASMUSSEN: Rod Rasmussen, não sou...

TARA WHALEN: Tara Whalen, advogada de privacidade do Google.

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.

ROY ARENDS: Roy Arends, principal cientista do APNIC.

JAMES GALVIN: James Galvin, SSCA, vice-presidente da SSAC.

PATRIK FÄLTSTRÖM: Patrik Faltström, presidente do SSAC.

RAM MOHAN: Ran Mohan, contato com a diretoria.

WARREN KUMARI: Warren Kumari, do Google.

JOHN LEVINE: John Levine, com afiliada sociedade da internet.

JEFFREY BEDSER: Jeffrey Bedser, ITreat.

GREG AARON: Greg Aaron, iThreat Cyber Group.

ROBERT GUERRA: Robert Guerra, Privaterra.

JULIE HAMMER: Julie Hammer não sou filiada a ninguém.

DANNY MCPHERSON: Danny McPherson, da VeriSign.

PAUL EBERSMAN: Paul Ebersman do Comcast.

CRISTIAN HESSELMAN: Cristian Hesselman do .registry.

PATRIK FÄLTSTRÖM: Muito obrigado a todos, nós temos três funcionários da ICANN, que nos apoiam. Então, o que nós vamos fazer é dar uma visão geral do SSAC, mostrar o trabalho que estamos realizando, o que vamos fazer no futuro e ver quais são as publicações desde a última reunião da ICANN e, finalmente vamos falar um pouco, vou falar com vocês que, a parte mais divertida de perguntas e respostas. E é por isso, é bom ter tantos membros do SSAC aqui, no momento são 31 membros, indicados pela diretoria da ICANN e fazemos recomendações e, questões relacionadas à segurança, integridade do sistema de anotações de nomes e números da internet. Então, por isso dissemos em vários relatórios que o escopo está relacionado à locação de nomes.

Temos diferentes especialidades em várias áreas e, como se vê nesse slide que, ainda não coube tudo aqui, fazemos muitas coisas... O que é importante aqui é que, quando indicamos os membros do SSAC queremos garantir o máximo possível que o SSAC, como um todo, tenha conhecimento necessário para escrever um bom relatório. Até agora nós temos 91 publicações e essa semana é a número 92, que foi distribuída, mas ainda não foi publicada, temos relatórios, recomendações e comentários. E é o que o SSAC acredita e temos todos os membros do SSAC e qualquer um pode falar de questões relacionadas a segurança, mas a opinião oficial é o que está no relatório. Os estatutos do SSAC estão ligados aos valores e missão da ICANN, que é garantir a operação estável e segura dos sistemas identificadores únicos da internet e, também preservar e melhorar a estabilidade, confiabilidade, segurança operacional e a interoperabilidade da ICANN. Nós trabalhamos com a diretoria da ICANN e, por isso, estamos ligados à missão da ICANN. Então, quando lemos uma recomendação à diretoria, nós enviamos as recomendações, a diretoria acusa o recebimento e estuda isso e pode fazer uma de quatro coisas, ou pode colocar essa recomendação no processo de elaboração de políticas, podem pedir que os funcionários implementem essa recomendação depois de um processo de consulta pública, podem publicar essa recomendação para as partes afetadas, ou podem decidir por uma solução diferente e explicar por que. A

ação formal não significa que a diretoria tem que fazer o que nós dissermos, mas fazemos a melhor recomendação possível, mas é claro que não é obrigatório, mas se isso não for feito podem haver riscos. Somos apenas um comitê consultivo e, todos devem ler as recomendações que fazemos e, se vocês acham que a recomendação é correta você a segue. Então, a recomendação tem força em si. Atualmente estamos, tem a ver com a harmonização do IDS, a gestão do espaço de nomes, gestão do risco de delegação de novas TLDs, isso tem a ver com o relatório da SSAC 90 e 91, queremos ver se é necessário fazer mais em relação a isso. Nós temos grupos de trabalho relacionados, as oficinas de DNSSEC e temos um comitê de emendas que avalia os membros do SSAC e potenciais membros que se inscrevem para participar do nosso grupo, desde a última reunião, quando publicamos documentos 85, 86, 87 relacionados... Desculpem, 85, 86 e 87 em resposta aos GTs de PDP do gNSO 88 e 89 são respostas ao ccNSO relacionados ao EPRSP do gNSO, o 90 são indicadores da saúde do sistema e o 91 está ligado a questão... 91 são os índices de saúde, indicadores de saúde e o 92 será publicado, é sobre direitos humanos. Então, se olharmos o que vai acontecer nos próximos anos, então o que nós esperamos... Algumas coisas de 2016 ainda ficaram para trás, na Q1-2017 ainda não foram publicados e, no Q2 seria uma oficina do DNSSAC na ICANN 59 e outras coisas, gestão do espaço de nomes e a nova rodada de gTLD. Se nós

olharmos em detalhes as publicações, desde a última reunião da ICANN e fomos de frente para trás, em tão revisamos os indicadores de saúde, de tecnologia de identificadores e descrevemos as cinco doenças que poderiam afetar a saúde da parte de nomes do sistema de identificadores únicos da internet e fomos o projeto da ICANN várias vezes, também discutimos o projeto essa semana inclusive, temos alguns problemas, em primeiro lugar com a escolha da tecnologia que foi atualizada um pouco, mas temos alguns problemas com falta de uma diferenciação entre coleta de dados e concluir sobre os dados no SSAC 90 fizemos uma recomendação sobre estabilidade do nome... O espaço de nomes de domínio, fizemos observação e recomendações para mitigar riscos claramente identificados, no 88 e 89, esclarecemos algumas questões que foram levantadas no 84 relacionadas ao processo do IPR, relacionados a avaliação que foi uma falha na identificação do processo de face track do ccTLD da IDM haviam problemas de confusão no relatório e esse relatório está ainda em andamento entre o ccNSO e o SSAC. Quanto ao SSAC 89 tivemos várias reuniões, entre o ccNSO e o SSAC, inclusive essa manhã, então há um progresso nesse tema. São alguns exemplos de perguntas que fazemos de como priorizamos nosso trabalho, como abordamos as solicitações da Diretoria da ICANN da comunidade e pediria que, qualquer um de vocês venha ao microfone e façam as perguntas que vocês querem. O SSAC escolhe o que vai trabalhar sozinho, a diferença

é que se uma pergunta da diretoria da ICANN, uma solicitação da diretoria da ICANN isso é priorizado, porque a nossa principal tarefa é fazer recomendações para a diretoria. Se as consultas públicas com prazo, então nós tentamos publicar o relatório dentro desse prazo e temos tido bastante sucesso nesse sentido. Nós também respondemos perguntas e fazemos recomendações com base em questões enviadas por outros membros da ICANN e no ano passado não houve nenhuma solicitação de avaliação de problemas, eu acho que seria muito importante ter, porque a última vez, o que nós investigamos fomos nós mesmos que identificamos, então nós também decidimos o que trabalhar sozinhos, lendo as listas de e-mail e vendo o que aparece. E como é que a comunidade pode monitorar a resposta da diretoria às recomendações do SSAC, isso tem sido acompanhado manualmente, historicamente e não tem funcionado muito bem e nós acordamos com a diretoria que isso não é bom, então a diretoria está desenvolvendo um tracker das recomendações à diretoria, ou seria um monitor e utilizam uma interface que ainda não está pronta, mas o maquinário por trás disso está pronto e nós, do SSAC e outros que querem saber como é que as nossas recomendações estão... Em que ponto está do processo, esse relatório pode ser solicitado, outros comitês consultivos também podem fazer isso. Como que o SSAC informa, como ele da de seu trabalho, por exemplo, um dos casos é como agora,

mas também nós publicamos os relatórios, o que é o mais importante, nós temos a página na internet, em que publicamos nossos documentos, temos as estatísticas, número de visitas e também das páginas da ICANN, que incluem o SSAC e vemos que é bastante consultado. E isso é muito bom, eu acho que todos os que vão para nossa página de documentos passam uns 03 minutos na página, o que eu acho bastante bom. Nós também temos uma conta no Facebook, também tentamos fazer alguns vídeos que são publicados junto com a equipe de comunicações da ICANN e, é claro, estamos tentando melhorar a nossa participação em outras reuniões, mas sempre que há uma conferência nós temos vários membros do SSAC que podem fazer apresentações, vivem em várias partes do mundo e podem fazer solicitações para que nós apresentemos esses nossos relatórios. Eu gostaria do Duncan e sua equipe, por nos ajudar a saber como comunicar as nossas ideias e nosso trabalho. Então, como é que a comunidade pode monitorar a resposta da diretoria às recomendações do SSAC. Bom, eu já mencionei isso, não é fácil fazer isso sem solicitar a equipe da ICANN, mas é isso que nós temos no momento. Então, eu quero passar a palavra para vocês. Então, esse é o feedback que eu queria dar para vocês, eu gostaria de abrir então para perguntas. Bom, façam a pergunta que vocês quiserem e vamos tentar responder. Bom, eu vou... Gostaria de saber se alguém do SSAC quer levantar alguma coisa? Mas é verdade, temos dito nos últimos 06 a 09

meses, há vários ataques que estão atingindo grandes proporções a internet de coisas, está se tornando enorme. Não é essa internet que nós queremos, o que vamos fazer contra esses ataques. Esse... Por favor, alguém da plateia pode vir ao microfone? Você pode ser membro... Alguém? Ótimo, Excelente.

JONATHAN MAKOWSKI: Muito obrigado pelo trabalho que vocês fazem para a comunidade. Algumas coisas que eu gostaria de levantar e receber o feedback um do DNS sinkholes e se deveria vir alguma diretriz da comunidade quanto ao uso de sinkholes ou quanto a imprecisão do WHOIS eu sei que o Governo Suíço está trabalhando com legislação sobre isso, eu gostaria de saber se isso é algo importante para a comunidade do seu ponto de vista. Eu tenho outras perguntas.

PATRIK FÄLTSTRÖM: Alguém aqui está trabalhando com isso?

ROD RASMUSSEN: A gente conversou sobre isso antes, isso na verdade, o tópico do sinkholes foi, na verdade, uma parte que fracassou há um tempo atrás, eu não sabia que isso ia surgir. O que é um DNS sinkholes, o conceito é de que se o nome de domínio está sendo usado para malware comand and control então ou usar esse site

para usar as instruções, então o que acontece, se você é uma empresa de segurança ou forças da lei, esses domínios podem ser retirados pelo registrador ou colocados de volta para registrar... Para que possa ser registrado novamente e pode-se ter uma combinação com o registrador para retirar esse nome de domínio e colocar no que se chama um sinkholes. Então, os computadores vão tentar chegar a esse mesmo servidor e, através das comunicações se pode saber quais são os computadores infectados e, dependendo do seu objetivo, os ISPs podem saber disso, as empresas podem saber disso, você pode usar para pesquisa, algumas empresas fazem todos os seus negócios com base nesse negócio e vendem essas informações para violação, uma vez houve uma empresa de segura que, os registradores, roubando sinkholes de outras empresas de segurança. Então, esse tema permanece importante e há um outro exemplo de sinkholes, em que se escrevem DGA que é um algoritmo o que acontece com o DGA, o mais, um dos mais... O exemplo mais famoso que foi o que aconteceu, que o algoritmo tem uma lista de dezenas a milhares de nomes de domínio que podem atingir e que usa comando e controle, então eles não precisam controlar um domínio que já existe, eles podem então dominar isso ou ter isso muito antes, mesmo antes dos domínios serem registrados. Então, isso parece ser meio, não está bem controlado. Então, isso pode ser chamado para controlar o último recurso do registrador, então

várias empresas de segurança pesquisadoras podem usar esse último recurso para colocar esses domínios tóxicos e estabelecer regras para o seu uso. E vocês devem ter ouvido sobre a avalanche que aconteceu, que iniciou em 2008 e a maior parte dos afetados se deram conta muito tempo depois, então há trabalho, então... Sendo realizado em relação a esse cybercrime.

DANNY MCPHERSON:

Eu concordo com isso, nossas atividades operacionais como quando fechamos alguns sites e também o Ransomware e todo tipo de delito cibernético e, quanto a privacidade da minha base de nomes, o fato de navegar na internet livremente pode levar a atividades maliciosas, fazemos o que podemos nessa comunidade para proteção dos consumidores. E o registrar é o último recurso ao qual podemos acessar, mas tentamos ser mais eficientes também, o grupo de trabalho e segurança política também, com outras ações de frente para proteção do consumidor. E outro recurso, uns documentos que foram feitos sobre como funciona a internet, são resumos que esclarecem com muitas informações, que estão sendo compartilhadas na internet e em cooperação também com as forças policiais. Então, isso é, estamos tentando ter um impacto estratégico de mais longo prazo, mas existem outras preocupações, como proteger infraestrutura operacional, com firewalls e outros

instrumentos e identificadores para proteger os endereços de IP, identificadores, assinaturas que cada vez são menores e que, talvez se queimem e já não possam ser mais utilizados e devemos limpar isso. Muito importante para a infraestrutura do ponto de vista operacional. Há muitas coisas que estão sendo feitas, estamos tentando ajudar com pessoas da VeriSign e ICANN com diferentes capacidades de contratar, também da segurança, operações e registros, etc. Para lutar contra esses delitos e temos, nos reunimos com grupos de trabalho e cada vez essa situação está ficando mais problemática com espaço de nomes e domínios, é um desafio. Muito obrigado.

PATRIK FÄLTSTRÖM:

Obrigado Danny. Infelizmente, esse SSAC número 01, que está funcionando com o registro de... Que saiu do ar não está aqui, infelizmente se ele estivesse aqui poderia explicar de melhor como foi essa situação.

DAN YORK:

Não é uma pergunta, você mencionou uma nova lista de atividades em andamento agora e há uma atualização que eu queria dar para informar às pessoas, havia 100 pessoas nessa reunião durante o dia, houve uma série de apresentações que eu insto as pessoas do SSAC para assistir pela internet, um painel de desdobramento de SSAC com ponto de cá e diferentes países

da União Europeia que estavam presentes, também uma sessão sobre ISP's. Paul Ebersman estava lá representando a Comcast, explicando que o ISP's estavam fazendo. E tivemos alguns termos e apresentação, sobre como DNSSEC para a segurança de e-mails. E uma das partes mais interessantes que surgiram daqui é que tivemos pessoas trabalhando em diferentes projetos que explicavam como esses projetos funcionavam bem melhor juntos e combinados. Também pessoas de estatísticas da SURFnet que fez uma apresentação muito interessante sobre o desdobramento de ISD e isso foi muito bom. E Jeff, seu pessoal veio várias vezes e Roland também fez um grande esforço de coordenação para falar sobre validação do DNS a medida que vamos aproximando do 11 de julho com um novo key being. E também houveram gravações, temos gravações, os slides também, eu quero agradecer novamente o DNSSEC sobre essa contribuição que foi muito valiosa. Muito obrigado.

PATRIK FÄLTSTRÖM: Não temos intenção ainda... Não temos intenção de finalizar essa cooperação, vamos continuar com ela.

MARIA HALL: Eu sou membro do RIPE e eu quero também unir-me ao que disse o comissário da Suécia, queria pedir que explicasse mais um pouco, qual é seu nome, senhor?

ROD RASMUSSEN: Rod Rasmussen.

MARIA HALL: Por favor, você poderia explicar mais profundamente sobre o que, como que o desenvolvimento da internet das coisas e como isso está relacionado com o que você estava mencionando ou não relacionado. Queria ouvir um pouco suas ideias sobre isso. E como parte do capítulo sueco da SSAC eu quero comentar que tivemos uma reunião, uma assembleia geral e alguém falou sobre uma regulação ou legislação e eram requisitos técnicos para todos os provedores, que fosse quem vende escova de dente, refrigeradores, qualquer coisa. E não sei se você ouviu falar sobre isso.

PATRIK FÄLTSTRÖM: O que nós temos observado no SSAC e temos aí no relatório, ainda não sabemos a quem dar a recomendação, o progresso enorme a respeito de internet das coisas, de que as pessoas compram, conectam, não as tocam mais. As pessoas não atualizam o software delas, há muitas coisas em que nem é possível fazer um upgrade do software e essa é outra área de interesse. Quanto a legislação, isso é como contar as pessoas que... Falar com criminosos, falar para eles: “Vocês não podem

entrar nas casas dos vizinhos.”, e não se se Danny você quer mencionar alguma coisa?

DANNY MCPHERSON:

Sim. Sua pergunta foi muito justa, tivemos esse painel e os operadores e registros que trabalham vários passos no ecossistema, infraestrutura, indiferentes do lado de recepção em que podem sofrer um ataque, sempre levamos isso em conta com muita seriedade para colaborar e preservar a integridade da infraestrutura. E falando com redes, navegação e, para isso, é preciso que vocês confiem e, sabemos que há danos que é problemático, portanto as parcerias que trazem a ICANN e também as comunidades de segurança operacional são muito importantes. Também eu queria voltar para o SSAC 04 e alguns dos ataques ao IT também e também na Tailândia, algumas atividades da DDoS são alguns exemplos em que havia também criptografados e também protegidos e então esse é outro aspecto. E quanto a segurança operacional eu não sei o quanto isso consome a ICANN ou outras comunidades, mas há alguns frameworks e uma série de pessoas como a (ininteligível) envolvidas com esse tipo de atividades, pelo menos nos Estados Unidos e também... É o que se chama de melhores práticas. E há muitas coisas que devemos tentar continuar melhorando enquanto a segurança e também fazer controles e contratar especialmente quando é necessário e com a mitigação e espaço

de nomes e espaço de números também da internet. Então, investimos muito em treinamento, contra-ataques DDoS e parcerias, aumentar capacidade. Sempre estamos adotando medidas antecipadas. Se temos a falha de mercado muito importante para software e hardware, não há mercado para hardware de qualidade, são os softwares de qualidade. Há coisas que são muito baratas, de má qualidade. O canal de provedores é muito efêmero e nós temos botnets muito ruins, temos o (ininteligível) e temos utilizado isso por 30 anos e sempre vídeo-câmeras que é muito mal, são mecanismos muito ruins e não podemos resolver isso. E o que observamos é que há dois protocolos que hoje funcionam com internet, só dois o HDTPS e o IDNS, para que sintamos que botnet, e o DNS eles podem lidar com os botnets e o DNS está presente, sempre ajuda e funciona. Então, podemos fazer com que o DNS destaque quando há esses problemas e interfira entre esses canais de controle, isso tem a ver com as pessoas, o lado do abastecimento enorme, há muitos dispositivos, sete bilhões de fato a cada ano de novos, entrando, e o que podemos fazer, podemos esperar fazer alguma coisa produtiva para tentar encontrar, entender esses canais de controle. Estamos tentando, não sei se estamos ganhando, vencendo, mas estamos tentando.

PATRIK FÄLTSTRÖM: Rod.

ROD RASMUSSEN: Realmente, eu vou... Eu quero falar sobre os problemas fundamentais aqui, o Geoff mencionou isso bem, que quando pensamos na internet das coisas vemos que é mais coisas na internet do que tínhamos antes, o problema é maior do que antes e temos alguns problemas. Um é a escala, em que temos um problema de magnitude para os próximos anos e esse é um problema. Outro problema é o uso incorreto de tudo isso, uso incorreto de positivos e isso faz parte também do problema dos fabricantes, não só as companhias de software, mas outras coisas, como bibliotecas que incluem coisas que não deveriam incluir em termos de tecnologia e não usam boas práticas. E durante todos esses anos nós temos lidado com a Microsoft para uma questão de codificação e de segurança e eles têm feito um bom trabalho, a Microsoft, mas há muitos dispositivos, e isso aumenta os problemas, e também há muita normalização, então pensem em todas as coisas que podem ser feitas do lado do abastecimento. Há analogias no mundo real? Sim, mas eu acho que não vamos resolver as questões do ponto de vista dos dispositivos, é mais vistos do que humanos no planeta, e isso é, mas há pontos de controle, pontos de acesso, há coisas que podemos fazer para fortalecer a infraestrutura, coisas que estão conectadas com a internet de maneiras que não deveriam estar

conectadas, e devemos falar com as pessoas, e são essas coisas que devemos fazer, há poucas pessoas que estão fazendo isso, e há pouco que, o que nós devemos fazer os operadores, as (ininteligível) da Google Control Networks, por exemplo, então ainda há esperança de que isso possa diminuir um pouco. Não sei, temos alguém aqui que quer dizer alguma coisa. Não sei se ele quer dizer alguma coisa ou não.

WARREN KUMARI:

O termo “internet das coisas” pode incluir qualquer coisa como definição, mas como disse o senhor são muitos dispositivos novos feitos de maneira mais barata possível para poupar muito dinheiro isso feito por pequenas companhias que não tem software, ou que o software não é a sua principal competência ou tecnologia, e que unem, montam uma série de coisas e eles esperam que elas funcionem. O BCPs acho que não vai resolver nada, e essas companhias não servem as melhores práticas ou tentam ganhar dinheiro, então acho que não haja muito controle do lado da cadeia de abastecimento, ou tentando também fazer um perfil dos dispositivos, porque não vamos conseguir nada. Muitas vezes é muito difícil agir a partir dos dispositivos, então o profiling é algo que pode não funcionar, também podemos agir sobre o CPE, as pessoas em geral, fabricantes, não escrevem seu próprio código pelo CPE, eles pegam alguns pedaços de software, como, autômato outras, o

que é o CPE, são os equipamentos produzidos pelos clientes, ou para os clientes como firewall, e há pessoas que pegam isso desde o início e mudam a página inicial, etc., com o código aberto e o framework é um conjunto de ferramentas que permitem que as pessoas possam construir um dispositivo IoT, e eles descarregam os softwares, selecionam os módulos que desejam, colocar o logotipo deles, e agora eles ficam assim dessa maneira, e isso fica bem mais barato do que fazer algo desde o início. Temos framework por exemplo que os fabricantes podem utilizar, e tem um incentivo de utiliza-lo porque isso é mais barato do que fazer a coisa desde o zero. E é isso que nós devemos observar.

NÃO IDENTIFICADO:

Muito obrigado, eu quero continuar aqui a discussão porque no outro extremo, há 25 anos, eu vejo que a questão da segurança naqueles dias, não era tão séria, mas hoje temos a experiência que é dispositivos que agora sim a gente pode colocar um parche, ou remendar por exemplo, e a gente hoje, há muitas coisas que não pode remendar, como Raio-X por exemplo no hospital, porque há uma série de proibições para fazer isso, é um requerimento, e segundo você falou sobre a segurança do HTTPS, mas sim os clientes querem interceptar, eles querem ver isso, e pode ter muitos firewalls por toda parte para, e com tantos ataques, as vezes eles veem a luz verdade e é uma

interceptação. Quanto ao primeiro problema, se houver cumprimento e licenças, como você disse, é outra parte do quebra-cabeças, e isso é um dos motivos porque o presidente do SSAC acha que nós não sabemos onde começou o problema. É muito difícil concentrarmos nesse aspecto de onde nasceu tudo isso, e tentamos dar recomendações para melhorar o mundo um pouco, porque exigir relatórios sobre problemas de internet das coisas é algo fácil, aqui nós, entre todos nós é provável que agora nessa hora, escrever matérias de, 50 páginas de matérias, mas realmente agir é difícil. Quanto ao segundo aspecto, se você menciona sobre as conexões TLD em SSAC, emitimos uma série de recomendações sobre como fazer certificados de maneira mais eficiente, também certificados com CA mecanismos, e também temos respondido ao ITU-D que é o contato com diferentes partes que pensavam que seria uma boa coisa lançar novos CAs no mundo e a nossa resposta foi que não, que era de uma maneira contrária, e também falamos sobre o DANE que mencionamos antes, e então o SSAC acha que as conexões dos TLDs e esses túneis criptografados deveriam continuar sendo end-to-end e utilizar determinadas terminologias similares. Talvez acham difícil de encontrar todos nossos documentos, mas de nós, temos todos os documentos' e veremos que há um fio condutor entre todos eles. Alguém mais?

NÃO IDENTIFICADO: Eu sou da Universidade de Oxford, eu queria saber o que, que vocês estariam interessados em pesquisa com a segurança.

GEOFF HUSTON: Eu também faço muita pesquisa, e os meus projetos em especial, é olhando de fora para dentro, é fácil medir essa estrutura, é fácil ter um laboratório, mas é difícil para mim ser eu e os outros bilhões como você, e que usam a internet da forma com que vocês veem. Tivemos sucesso em algumas áreas, especialmente nos projetos de medição da penetração do IPV6, em todas a internet, quase em tempo real. E também introspecção do Sistema de nomes de domínio, vemos quantos usuários mundiais, não vão para o nome do domínio, se ele não for bem assinalado pelo DNSSEC. Isso é um bom sinal, então eles querem saber a diferença entre o que é verdade e o que é mentira. Há muita validação do DNSSEC, na Austrália, no meu país, há muita diferença entre países e entre provedores. Então esse tipo de coisa, então o que, que, como se vê a internet de fora para dentro? Porque a internet somos todos nós, não somos só os pedacinhos no meio, são os que estão por fora.

WARREN KUMARI: Então, seguindo, como é que a internet em diferentes países, entender melhor que coisas podem ser atingidas ou não? Há censura ou esse tipo de coisa, por que, que eu não consigo

entrar em alguns sites, em alguns países, e o que, que eles fazem por causa disso, ou para que isso aconteça?

DANNY MCPHERSON: Eu tenho visto muitas pesquisas interessantes sobre dependências de sistema, como o trânsito e gráfico de confiança, o uso da nuvem, eu acho que 300 ccTLDs e 60 não tem uma única autoridade que trabalhe com isso. Então depende de operações no cyber espaço, e esse é o tipo de coisa, há uma estrutura de multiutilização, multiusuários, então alguém tem o impacto em algum lugar, e isso pode afetar milhares de empresas. Eu acho que as coisas vão ficar cada vez maiores, e cada vez piores por causa das questões da nuvem de confiança de trânsito e tem a ver com a estrutura mais ampla da internet, interesses de estado e resiliência e continuidade empresarial é muito importante, e o que, que afeta isso deve ser pesquisado.

CRISTIAN HESSELMAN: Uma outra pesquisa é que os usuários tenham maior controle da segurança dos seus dispositivos relacionados à questão de IT que tivemos, então se houver vulnerabilidades de segurança, vão tirar esse dispositivo da rede, e vão se proteger, protegendo também a estrutura do DNS. Outro tema como é que os operadores e outras partes interessadas compartilhariam os

seus dados, e levando em conta a segurança disso, nessa discussão o que nós fazemos é agrupar as coisas em classes que são fáceis de medir, e identificar, como por exemplo, países. Um outro estudo interessante que o SSAC poderia fazer, é medir as categorias que não estão sendo levadas em conta, como as AS há monta por exemplo, os países podem ser um, a realidade não segue o código de país, mas isso ainda é um padrão de medida, o que há disponível, e temos que pensar nisso talvez aqui, eu não sei se a gente pode pensar em escola primária ou universidade, mas me parece que há várias outras métricas que poderíamos utilizar além de país.

GEOFF HUSTON:

Olha, isso muito quando se vê o roteamento, números autônomos, são outro identificador chave, então quando você publica por país, muito mais gente lê a sua publicação, ou do que você publica pelos números autônomos. Então a gente faz de acordo com o que os leitores querem ler.

NICK SHOREY:

Eu sou do governo britânico, nós recentemente começamos a ver o IRT e essa segurança por padrão, e estamos pensando na viabilidade disso. E uma das coisas, que eu queria saber é o que você faz, quando a gente entra nessas áreas cinza, são quanto esses dispositivos se tornam obsoletos, e algumas empresas não

tem como a sua parte forte, IoT, então eles vão no mercado e compram já uma coisa semi pronta. Então eu gostaria de saber, talvez não agora, de ideia para solucionar essa questão, quando há muitas coisas online já estão obsoletas, então há alguma pesquisa que eu possa levar para o meu governo?

WARREN KUMARI:

Eu acho que eu não tenho uma boa resposta, eu sempre busco pontos de acesso para a minha casa, e eu quero sempre que sejam baratos, e eu fui no Alibaba, que é um enorme mercado, encontrei 700 empresas diferentes que vendem exatamente os mesmos dispositivos então você compra 400, os faz mais 400 baseados nesses. Então não faz sentido atualizar esses dispositivos, é mais barato construir novos, então uma opção possível, que eu acho que fez o Linksys alguns anos atrás, então você compra um roteador que funciona por dois anos e misteriosamente a fonte queima, então você tem que comprar outro. Então quando as coisas são muito baratas, elas acabam se tornando obsoletas, e estraga, e você compra uma outra.

ROD RASMUSSEN:

Eu acho que é muito pior, e o que, que você faz com quem vende os seus telefones, Smartphones, como é que você muda as senhas, e o que é bom saber é que há muito progresso nessa área, está sendo feito trabalho, há marcos para abordar essas

questões, as pessoas não estão tentando dizer: bom, essa é uma pergunta padrão pros fabricantes, essa é só uma ideia de regulamentação, mas funciona as vezes, nem sempre estamos de acordo com tudo no SSAC entre nós, mas há alguns esforços em relação à isso.

ROBERT GUERRA: Eu gostaria de seguir o que o Warren disse, eu sugiro ver o turris.nz, fala de roteador, código aberto, é uma iniciativa interessante que tem esses dados que você poderia compartilhar. Há iniciativas em outros lugares também, então é isso que eu gostaria de lhe informar.

PATRIK FÄLTSTRÖM: A última pergunta de hoje.

JAD EL CHAM: Eu sou Fellow da ICANN, em primeiro lugar agradeço as suas respostas. Eu tenho uma pergunta que já faço há três dias, mas não consegui nenhuma resposta, a gente ouve falar da internet das coisas, ataques ao DDoS, mas há novos ataques de DDoS, esquecemos os protocolos que são usados quando se fala de DDoS, se fala muito de DDoS refletores, o que então empregamos então segurança para os nossos clientes, o SSEC, aborda essas falhas, de segurança, podemos usar esse DDoS,

como refletores do DNS, ameaça do DNS? O IETF está lidando com isso, eu sei, mas eu gostaria de saber se a ICANN está envolvida nesse tipo de atividade?

PATRIK FÄLTSTRÖM:

A ICANN em si é como muitas organizações, opera infraestrutura de TI e operam também na raiz como nós e o Google também, e muitos de nós participam com outras organizações para estabelecer melhores práticas e trabalhar com esses protocolos que são os mais populares, e usa-los para combater os ataques. Em geral, os endereços de IP e spoofed, há vários botnets configurados, alguns dos botnets são grandes e difíceis de encontrar, e as vezes a gente não consegue fazer o spoofed do endereço de IP, não é NTP, essa questão do press, e não é nenhum tráfego comum, alguns ataques de reflexo que estão usando a amplificação a melhores práticas para configurar o servidor de NTP e então alguns ataques não são conhecidos pelo servidor de NTP, a ICANN opera essas coisas e, portanto, ela participa. Quando ao processo de elaboração de políticas, há diferentes mecanismos, tanto do lado das partes contratantes quanto contratadas, e esse tipo de coisa é levado em conta quando levamos em conta as exigências das partes contratadas e de melhores práticas. Mas quando a questões operacionais, a resposta é que nós que participamos da comunidade da ICANN,

também participamos dos fóruns em que essas questões operacionais são discutira. Warren você quer falar algo?

WARREN KUMARI:

Você está falando especificamente são ataques de reflexo, e eles têm a capacidade de fazer o spoof de endereços fonte. Então, há uma mulher prática para isso, e eu acho que o SSAC 004 que diz a mesma coisa. A ICANN não pode fazer muita coisa com relação a isso. Quem é que tem esse programa? Eu acho que o ISOC ou MANRS, ou que seria modos. São coisas que se pode utilizar, a empresa pode utilizar que seguem ou que tem boa educação, tem boas maneiras, e infelizmente a ICANN em si não pode fazer muito em relação a isso, a ICANN não tem nenhum poder contra as ISPs, a não ser quando a ISP pode dizer que não vamos dar, fazer contratos com ISPs que não tem proteção contra spoof, mas isso já acontece há bastante tempo. Muito obrigado.

PATRIK FÄLTSTRÖM:

Muito obrigado a todos, são 16:15, muito obrigado por virem, então parece então que a nossa reunião às 15:15 é mais popular que aquela reunião que a gente fazia às 8 da manhã, muito obrigado.