SAN JUAN – Como funciona: Informações básicas sobre abuso do DNS
Segunda-feira, 12 de março de 2018 – 13h30 às 15h AST
ICANN61 | San Juan, Porto Rico

PESSOA NÃO IDENTIFICADA: Boa tarde, ICANN 61. Como funciona: Atendendo o abuso no DNS.

CATHY PETERSEN: Boa tarde. Em breve vamos começar a sessão de como funciona, ou como entender o abuso do DNS.

Boa tarde a todos. Vamos ver essa sessão de como funciona: como entender o abuso do DNS. Temos Carlos Alvarez do diretório técnico, que vai apresentar.

CARLOS ALVAREZ: Obrigado a todos. Eu sei que há 23 participantes online, então vamos iniciar a sessão.

Vamos falar então de um tema que é muito importante. Realmente pertinente. Também é conflitivo em alguns aspectos. E acho que todos têm que prestar atenção a isso, porque vamos falar sobre o abuso no DNS.

Em primeiro lugar, vamos estabelecer de que vamos falar exatamente, porque há diferentes formas de entender o que é o abuso do DNS e há diferentes perspectivas. Falaremos sobre elas, daremos exemplos do que é o abuso, o uso indevido do DNS.

Depois vamos falar de como evoluiu todo esse panorama quanto as ameaças do DNS, e depois vamos finalizar falando sobre o abuso do DNS no contexto da ICANN.

Primeiro que foi mencionado é que não existe uma definição aceita internacionalmente do que é o abuso do DNS. Como diz a imagem, há diferentes variantes da definição. Algumas incluem o delito cibernético. Outros falam dos hackers, e outros de quando são alguns emails maliciosos.

Então se faz também uma diferença entre o que é o abuso do DNS, o uso indevido do DNS. O que diz a transparência é que o uso indevido faz referência a atividades não solicitadas, que podem ser conspirativas, e que fazem o uso ativo do DNS aos procedimentos para registrar os nomes de domínio. Depois vamos ver de que se trata.

O que disse o GAC, tentando chegar a uma definição, ou dar elementos para entender o que era o abuso do DNS, o que disse o GAC em realidade a essa área tão ampla. O GAC, em seu comunicado, ofereceu medidas de proteção para os novos gTLDs, e um enxerto desse documento fala da mitigação de atividade

abusiva. Fala de certa atividade abusiva ,como distribuição de software maliciosos, phishing, pirataria, violação a direito de autor e marcas comerciais, práticas fraudulentas, falsificação, ou que significa uma atividade contra a lei.

Isso é muito amplo, e alguns pensam que alguns dos temas incluídos aqui não representam abuso técnico do DNS quanto a protocolos técnicos do sistema. Mas, como disse, elas são diferentes visões da comunidade. Essa é uma. Principalmente quando fala em violação de direito de autor e marcas comerciais, ou práticas fraudulentas, enganosas. Não se considera tecnicamente abusos.

Há uma grande pergunta que vou deixar aberta durante a sessão, e tem a ver com se o Spam é ou deveria ser considerado um abuso do DNS, do sistema de domínio.

No lado de organismos de aplicação da lei, o Spam é um predecessor de outros tipos de atividades maliciosas, mas em si próprio, pelo menos até hoje, não foi considerado um abuso técnico do sistema de nomes de domínio global.

Quando estão fazendo então a pesquisa sobre ameaças e analisam dados, vocês podem ver que há uma campanha de Spam que foi lançada como para saber qual a infraestrutura, identificar a infraestrutura criminosa utilizada por esses setores para essa campanha. Se continuam com a atividade, finalmente

vão ver que existem outras atividades vinculadas que seguem depois dessa atividade. Pode ser distribuição de um material abusivo, phishing, diferentes tipos de coisas.

Para dizer de forma simples, o abuso do DNS faz referência a qualquer coisa que ataque ou abuse a infraestrutura do DNS, e há muitas formas de poder ver o abuso do DNS. Podemos falar de duas formas. Uma é a perspectiva do abuso da resolução dos nomes de domínio, que é a parte técnica de como os nomes de domínio se traduzem em endereços IP, e a outra perspectiva tem a ver com registros dos nomes de domínio. Eles são serviços que oferecem registros e registradores, e abuso por parte dos delinquentes de diferentes formas. E falaremos também sobre isso.

O uso indevido do DNS faz referência então a explorar o protocolo de DNS, o processo de registro de nome de domínio com fins maliciosos, e isso está exemplificado e explicado com mais detalhe mais para frente.

Não é necessário ler tudo que diz na transparência, porque o que quero mostrar aqui são os elementos operacionais de DNS. Em escala significativa. Em azul temos acima o que são os servidores de nomes de domínio qualitativo, que tem os que têm os dados são para cada TLD, para cada nome de domínio. Por baixo, encontramos os nomes recursivos que podem vê-lo como

servidores de DNS que é o ISP – que é o que vocês têm, que é o que fornece o acesso a internet – permite utilizar, dar um serviço de resolução de DNS, e depois temos o que são os resolutores terminais ao cliente.

Esses servidores são esses. É uma função dentro do meu navegador, por exemplo, que procura informação que precisa para utilizar os recursos que eu quero utilizar.

Por exemplo, vou para o navegador e coloco www.icann.org. Esse resolutor terminal vai resolver esse nome de domínio dentro de um endereço IP. E o conteúdo, onde está o conteúdo de ICANN.org vai fazer download no meu dispositivo, vou poder interagir, etc. Esses 3 elementos operacionais do DNS são objetivos de ataques. Alvos de ataques.

Bom, tudo é alvo de ataque em realidade, né? Vamos ver exemplos. Porque vamos falar então da reflexão e amplificação. Isso tem a ver com os ataques de DDoS que são os de negação de serviço.

O que é a reflexão? Reflexão significa que podemos enviar um pacote, falsificar informação sobre o endereço IP fonte para que o servidor pense que mandou outra pessoa. Temos esse servidor que envia uma resposta a esse endereço. Então se meu objetivo é atacar a Cathy, eu envio o pacote ao servidor do DNS, e o

endereço IP que vou incluir nesse pacote vai dizer que o pacote vem da Cathy, e não vem de mim.

Se eu usar os resolutores abertos que são servidores de DNS, que existem e há milhares deles, que não podem resolver as consultas dos endereços IP, e que estão resolvendo por outras partes do mundo, Cathy vai ter muitíssimos pacotes, porque todos temos esses resolutores que estão em toda parte, e então todos vão pensar que as consultas foram enviadas por Cathy, e todos vão responder a ela. Isso é reflexão.

O outro vetor é amplificação. Amplificação significa que todas essas consultas que estou enviando são pequenas, e em geral se trata de uma linha de comando. Essa linha pode ser tão simples como nome do servidor, nome de domínio. 7 bytes apenas, é pouco. Mas a resposta pode ser muito grande, 2.3, 2.7 megabytes, se deve muito implicar isso pelos milhares de consultas, eu estou fazendo com que meu botnet envie. Botnet são grandes redes de alguns dispositivos que podem manejar centenas de dispositivos comprometidos. Então o delinquente que estiver com botnet vai ter todos esses dispositivos comprometidos, que enviem consultas a esses resolutores para que enviem a resposta a Cathy. Há uma multiplicação.

Então isso tem a ver com os dispositivos que estão comprometidos, que eu já recrutei, são parte do meu botnet, pela

quantidade então de resolutores que eu estou potencializando, e envio o comando, envio essa consulta que sustenta a informação de DNS. Envio uma resposta e esse comando está, como disse, a consulta é pequena, mas a resposta é muito grande.

Então Cathy vai ter muitíssimas coisas, e pode ser infectada se não tiver algum tipo de segurança. Além disso, vai colapsar, se não tem forma de fazer frente a tudo quanto está chegando.

Acho que em 2003 foi utilizado então o DNS com o vetor que foi Spamhaus. Houve um ataque dessa empresa, que deu boa informação sobre o que era liquidação e proteção contra ameaças.

Obviamente os ataques evoluem. O DNS não é o único vetor, mas é um deles. Mas como protocolo, está sendo explorado.

Também temos o envenenamento do cache, ou o ataque de esgotamento, e depois o que é o ataque do intermediário do DNS. Depois vamos ver isso. Aqui.

Isso é basicamente o que eu eu acabo de descrever. Temos um ataque que usa a reflexão, porque envia pacotes que estão falsificando o endereço IP, então esses resolutores abertos pensam que é Cathy o dispositivo que estão enviando as consultas. A consulta que recebem é tal que engatilha uma resposta muito grande. Esse é o vetor de amplificação. Cathy

recebe toda essa quantidade de informação, que é o que eu acabo de descrever.

Esse não fui eu. Deixe eu ver. Acho que tomei bastante, bebi bastante café, por isso vou ser muito rápido. Vamos aqui. Outra forma em que se pode atacar o DNS. É através dos servidores de nome de alguém. Esses servidores dão resolução para um nome de domínio. Então seu eu digo carlos.oquefor e digo idealmente que tenho que ir a servidores onde o DNS é um sistema global, vai obter informaç~eos sobre os recursos que tenho associado a esse nome. Em outras palavras eu vou de definir, e vou colocar a disposição essa informação através de servidores de nomes, e endereços de IP onde está meu email, está o servidor de word, está o FTP. Então se alguém vai para meu servidores de nomes e quer falsificar não vai receber essa informação. Eu não vou poder receber correio eletrônico, não vou poder enviar email. As pessoas não vão poder acessar o meu website, etc. E pode haver consequências se estamos falando de um nome de domínio de valor. Não no caso de Carlos, que poderia ser.

Esse tipo de ataque faz um abuso delitivo do protocolo TCP. Quando envio um pacote de TCP ao servidor ele me responde, e isso é em termos muito simples, e responde ao endereço de TCP, tanto do dispositivo que iniciou a conexão, como aquele que responde, vão de mãos dadas.

Isso gera um canal de comunicação que mantém ambos. Ou seja, os 2 tem que alocar recursos para manter esse canal de comunicação. Se eu tenho muitos dispositivos comprometidos em um botnet e todos enviam respostas em consultas a um servidor de nome, de forma que fazer com que esse servidor estabeleça aproximações TCP demais, ou seja, muitos recursos para manter esses canais de comunicação estabelecidos através do TCP, chega a hora em que esse servidor não vai ter já recursos para alocar nenhuma conexão de TCP.

Ou seja, que ninguém vai poder pedir informação do DNS ao servidor. Vai continuar estando online, mas não vai poder responder nenhuma consulta.

Isso é o que diz aqui. Porque diz que se degrada, ou interrompe, a resposta. Se não podemos então resolver esse nome, em uns minutos, imaginem se estivéssemos falando de muito tráfego e o multiplicamos em milhares, quando falamos em nomes de domínio talvez percam totalmente a resolução do nome. Obviamente todos queremos evitar isso porque é o pior dos casos.

O envenenamento do cache. Isso é realmente ruim, porque os maus são muitas vezes criativos. Vocês se lembram que eu mencionei antes que temos servidores de nomes autoritativos na parte superior, e que o associamos em ns1 com carlos, ou o que for, para dar ao DNS com informação com o que é meu servidor de

rede, de correio. Esses são meus servidores de nomes autoritativos.

Depois todos os ISP e todos que estão ali, ou 8.8.8.8 ou 9.9.9.9, os diferentes fornecedores de DNS tem recursivos, ou seja, que fazem perguntas em nomes de outros.

Alguns desses resolutores discursivos não estão bem protegidos, são vulneráveis. Imaginem os milhares de ISP que estão ali em todas as regiões, alguns estão operados por empresas pequenas, que não têm recursos demais. Tem infraestrutura para operar, mas talvez não tenham recursos para se proteger. E quando esses servidores não estão suficientemente protegidos, os delinquentes podem devolve-los de diferentes formas.

Uma é eu ser um usuário do ISP que tem um resolutor recursivo comprometido. Envio a consulta, procuro dados vinculados com não sei, pro .com, então recebo a resposta correta, certa, mas como o servidor já está comprometido os delinquentes vão adicionar outra parte mais a informação, e essa informação vai dizer também o endereço de IP, para Bank Of America é esta. E o que eu faço é atualizar a memória cache de todos os meus dispositivos, que vai ser o arquivo host.

Quando isso acontece, o que vai acontecer com meu dispositivo a próxima vez que eu queria ir para o Bank Of America? Aonde que vai me levar? Isso aconteceu por um período de tempo, vai me

levar para o endereço de IP que os delinquentes queriam que eu visitasse. Essa é uma situação ruim, não é nada bom. O que vai acontecer então? Eu vou visitar o servidor operado pelos delinquentes, posso ver o conteúdo que eles querem que eu veja nesse caso, vai ser um site phishing que vai ser igual ao Bank Of America, e sem problemas vou passar meu número de usuário, e minha senha. Em realidade não vai ser bom para minhas finanças pessoais. Outras formas nas quais os delinquentes podem fazer coisas como essa, porque podem comprometer diretamente o dispositivo, e modificar a configuração do DNS.

Então, quando fazem, vermos depois em um exemplo, em um botnet. Aconteceu faz 8 anos eu acho, se o meu dispositivo estiver configurado para enviar consultas de DNS, por exemplo, 1.1.1.1, mudam esse endereço, e em lugar desse endereço legítimo colocam o deles. Colocam o próprio endereço que eles configuraram, que está configurado para dar o seu endereço IP para a estrutura. Em outras palavras, vão ter os usuários com dispositivos comprometidos, todos vão visitar seus websites. O que obviamente não é agradável, e depois vamos falar disso.

Em casos como esse, falando principalmente em envenenamento do cache, tem o dispositivo comprometido que envia consulta a seu servidor de DNS. Eu estou procurando um site que não é importante para os delinquentes, não sei, qualquer um, um que é novo. Mas esse site não é importante para os delinquentes. Como

fizeram no exemplo anterior que eu lhes dei, adicionam outra parte de informação na resposta, para que os servidores deles enviem ao meu dispositivo, e essa informação pode ser similar ao endereço IP. Ah, e também se quiserem, é o endereço para seu banco é esse. Então dentro de um período definido, eu vou fazer uma consulta para esse nome de domínio no meu banco, porque quero fazer banco online, e acabo com o website dos delinquentes. Novamente isso afeta minhas finanças pessoais.

O DNSChanger é exatamente o tipo de situação que estava descrevendo. Exatamente o que fez, mudou a configuração do DNS que pretendia o usuário. E foi muito abrangente. Utilizou esta botnet, as mentes mestres por trás dessa operação conseguiram ganhar muito dinheiro, para o qual nossas autoridades de aplicação da lei conseguiram descobrir, conseguiram demonstrar com contundência que tinham conseguido 25 milhões de euros de forma ilegal. Isso não significa que tenham ganho mais, apenas conseguiram demonstrar isso as autoridades como evidência.

Com o DNSChanger os criminosos mudaram a configuração do dispositivo do usuário, e fizeram uma coisa que parecia ser bastante inócua, porque substituíam as publicidades que vêm os usuários quando acessam o website. Então se eu entrasse em meu local de endereço de notícias preferido, de manhã no escritório, com minha xícara de café, não estaria vendo as publicidades legítimas, mas outras. Isso também levava dinheiro para eles de

forma contínua, e isso aconteceu durante muito tempo, então foi uma máquina de fazer dinheiro, não provocou danos, pareceria. Não se viu nenhuma conduta estranha nos dispositivos. Os usuários podiam acessar o conteúdo que viam, poderiam interagir e com os recursos que queriam. Então a simples vista não tinha nada errado, mas sim, por trás sabemos o que existe. Ou seja, se provocou essa ação, e houve tanto dispositivos emprestados, eu não lembro a quantidade certa, mas eram milhares de dispositivos que estavam comprometidos por este tipo de atividade maliciosa em muitos países. Poderia ser para 20 países, mas não tenho certeza da quantidade.

Então o pessoal se fez uma pergunta, que é, qual é o meio das autoridades? Então alguma coisa tinham que fazer, alguma coisa com esses DNSs com os quais os criminosos estão agindo. Podiam desativá-los, e o que teria acontecido se apagado? Se as autoridades cortassem os usuários pensariam que perderam a conexão com a internet, estariam conectados, mas os servidores positivos não trariam qualquer resposta.

Então o que fizeram, já que não podiam apagar, era utilizar engenharia para substituir esses servidores, e o administrador desses servidores, durante um tempo, utilizou diferentes técnicas e houve campanha de sensibilização, feitas durante diferentes jurisdições, para que os usuários soubessem que tinham que fazer uma limpeza, como análise de seus dispositivos.

Sendo que os criminosos encontraram diferentes formas de abusar do protocolo do DNS, e de utilizar para fins ilícitos os diferentes operações do DNS, é interessante, pelo menos da perspectiva acadêmica, ver que isso demonstra que atividade para fiz ruins, mas são criativos. Por exemplo, o canal de infiltração encoberto, eu acho que esse é o seguinte exemplo.

Aqui temos um canal de infiltração encoberto que se produz quando se enviam dados de uma rede comprometida, sem que o administrador da rede perceba que estão roubando seus dados. Essa é a parte encoberta. E o DNS é considerado um canal de infiltração realmente muito bom, como é coberto, porque há um ponto pequeno que se utiliza para o DNS, para as comunicações, e não pode ser bloqueado.

Então o tráfego nas redes se translada de um ponto ao outro, através desses portos. Os portos que utiliza o protocolo DNS é a porte 53. Enquanto os engenheiros podem atribuir essa porta da rede, podem gerar algumas complicações. Então geralmente não se volta a atribuir para outro ponto. Isso significa que o tráfego pelo ponto 53 não pode ser bloqueado, é muito difícil para depois redistribuir. Não pode ser bloqueado. Isso tem a resolução do DNS, então vão pensar que está tudo bem.

Agora como funciona quando temos um canal de cooperação encoberta? De diferentes formas. Pelo menos há duas formas que

me ocorrem agora. Uma tem a ver com o que se compromete. Se faz o seguinte, se compromete um dispositivo, e esse dispositivo começa a enviar consulta de forma lenta, são servidor no nome dos criminosos, o que acontece é que dentro dessa consulta de DNS, os criminosos substituem os bits com os relevantes com aqueles que estão filtrando.

Então as consultas do DNS continuam sendo as consultas do DNS. Sem que a engenharia, ou o administrador da rede, analisando essas consultas no tráfego, vão ver que são consultas do DNS, mas vão ter que recolher todas essas consultas ao DNS que estão utilizando para a filtração desses dados específicos, vão ter que reunir e se requer muita análise. Tem que perceber de que há algumas peças que estão sendo substituídas, e tentar de saber o que está acontecendo e quais são os dados que se filtraram. Essa é uma forma.

Outra maneira na qual os criminosos utilizam o DNS para arbitrar os dados é através de registros, um deve administrar um arquivo de zona. Nesse arquivo, o nome de domínio, encontramos um recurso que está vinculado com esse nome de domínio, que se inclui a informação do website com o servidor de correios eletrônicos, e tem uma assinatura de DNSSEC, se tem outra tecnologias para proteger os clientes ou a rede pode estar ali também. Há mais siglas infelizmente, talvez escutaram falar de FTP, SPF, DKIM, DMARC, que se utiliza para proteger a rede. Todo

esse tipo de informação termina no que chamamos registros de textos. Podemos colocar qualquer coisa nesses registros de textos. Não há limitação quanto ao tipo de textos que podem ter esses registros de textos, apenas são textos. Então os criminosos utilizam desses registros para filtrar informações também.

Podem enviar consultas com informação do registro de texto a qualquer servidor que unem essa informação, podem reunir, recriar os dados que foram filtrados, etc.

E o fluxo rápido, eu acho que isso já foi mencionado.

Temos os registros dos nomes de domínio que são alvos atraentes para os criminosos. Infelizmente, há abusos cometidos nesse espaço. No espaço dos ccTLDs, adoram fazer abuso do registrador e dos revendedores, ter acesso a grande quantidade de nomes de domínio. E é um problema muito complexo para resolver. Com os preços mais baixos de nomes de domínios, tendem a estar vinculados com pessoas que atuam mal com a natureza humana, e aí eles podem vender esses dados. Os registratários e os usuários legítimos, muitas vezes buscam o preço mais baixo, e termina com esse nome de domínio que não são lícitos.

Este tipo de abuso das registrações faz parte de como evoluiu a indústria, e agora há muitos desses nomes, mas os atacantes abusam, e quando menciono essa situação estou pensando nos domínios DGAs, que são aqueles que estão nas mãos dos

atacantes para poder gerar montes desses nomes de domínio. É um algoritmo para geração de domínios.

Então utilizam uma infraestrutura, os criminosos, para poder enviar e controlar essa infraestrutura, e o que acontece se esta estrutura cai? Tem que ter um plano B, C, e D. Então em termos dos DGAs, quando a botnet se percebe que um desses servidores associados com o comando e controle está desativado, ou não está funcionando, gera, é só um exemplo né? Porque há todos os tipos de variantes de condutas de DGA, essa é uma explicação mais simplificada de como se utiliza esse algoritmo. Então se ativa uma nova cadeia de caracteres para esse TLD e se começa a funcionar.

Então se pode controlar essa situação na botnet por uma ação litigiosa, ou de ameaça, aí se perde a funcionalidade de controle e comando, por esse algoritmo se pode continuar funcionando.

Vou mencionar um exemplo muito interessante, espero estar chegando nesse slide. Porque os atacante de criminosos registram o nome de domínio? Para tudo que pensam, para substituir identidade, para ransomware, para malware, para vender produtos falsificados, para tudo aquilo que podem imaginar.

E a última aba que está aqui, que não sei porque não aparece, corresponde ao controle de comando, que tem a ver com a

capacidade e estabilidade que são as maiores preocupações com os ataques que estamos sofrendo.

As vezes há perguntas referidas aos produtos farmacêuticos ilegais, se isso tem que ser considerado abuso do DNS, ou se está vinculado tecnicamente com o abuso do DNS. Isso se parece mais a situação dos websites falsificados, e é verdade, mas as vezes há algumas coisas que sujassem por baixo da superfície. Não posso entrar em todos os detalhes agora, mas levem em consideração que há algumas coisas que estão por debaixo, e você vê na superfície. Talvez vocês vêm que apenas se trata de websites utilizados para enviar de forma ilegal algum medicamento em lugares onde está proibido, mas muitas vezes, por baixo dessa superfície, há outras águas.

Tem alguma pergunta? Se aproxime, por favor, até o microfone.

CATHY PETERSEN: Pode utilizar qualquer.

FARZANEH DABII: Eu sou Farzaneh Badii, sou presidente de partes interessadas e pergunto a título pessoal. Quando dizem por baixo o nome de domínio que vendem medicamentos de forma ilegal, podem haver outras situações, estão falando de algum abuso de índole técnico ou estamos falando de conteúdo?

CARLOS ALVAREZ: Estou falando de operações criminosas, que podem utilizar esse nome de domínio. Tem a ver com o conteúdo de web, e a atividade criminosa que continua por aí.

FARZANEH DABII: Então isso não tem nada a ver com superstições técnicas do DNS?

CARLOS ALVAREZ: Tem a ver com o uso do nome de domínio.

Então por que vão pagar os criminosos pelos nomes de domínio, se eles podem roubar ou controlar de alguma outra forma? Há diferentes situações nas quais os criminosos podem se aproximar desses nomes de domínio, e não apenas sequestrar um domínio, como fazem?

Podem comprometer o uso das habilitações, talvez os acessos aos registratários através do painel, que é a interface que permite aos registratários administrar o seu nome de domínio. Imagine uma organização de criminosos que querem tomar o controle do nome de domínio de muito valor, ou querem provocar danos aos clientes de um banco específico. Podem talvez enviar uma campanha de substituição de phishing, podem encaminhar aos funcionários do banco depois de algum trabalho de engenharia

social, podem atrair os empregados com cenários que cliquem em uma parte indevida, e aí podem roubar talvez sua habilitação, ou senha de acesso.

Depois desse ponto chega até onde eles, como criminosos, querem. Podem criar um domínio de terceiro nível por baixo do de segundo nível. Se o banco sofrer uma situação desse tipo, o banco de carlos.nãoseioque, o criminoso pode criar um endereço semelhante a outro nível, pode enviar um email como parte de uma campanha de phishnig, atrair as vítimas bem sucedido, porque nomes de domínio de segundo nível é o meu nome de domínio real. Pode modificar dos servidores de nomes, ou qualquer outra informação que esteja associada com o nome de domínio. Podem modificar os registros, podem dar baixa a todos os registros, e podem colocar o próprio arquivo para esse nome.

Há situações onde os registradores, que talvez não tenham sua infraestrutura bem protegida, se viram comprometidos. Não é o que aconteceu muitas vezes, mas aconteceu. E quando acontece não é uma boa situação. Felizmente são poucos casos que vimos, os criminosos apontaram arma branca de alto volume, muito específicos, e os registradores conseguiram responder altamente, isso aconteceu há um tempo atrás, e se manejou de forma adequada.

Mas os criminosos procuravam buracos específicos, alvos específicos, para dominar alguns servidores. O registratário, por sua vez, é atraído a clicar e uma coisa indevida por meio de um ataque de phishing bem sucedido, ou através da estrutura de registração, ali podem ter sucesso.

O que estava mencionando antes, esse outro aspecto do phishing. Os registratários, quantos deles poderiam ter habilitação de acesso para o painel de controle para administrar os nomes de domínio. Quantos registratários vão ter as mesmas habilitações, ou senha de habilitação, para esse painel de controle, como em uma conta que tinha se comprometido antes.

Em qualquer uma dessas situações, todos os meses ou semanas temos essas situações, agora quantas são desconhecidas. Os criminosos tentam conectar a tantos servidores quanto podem, com nome de usuário e a senha que foram roubadas de outras violações a segurança. Quando a seleção já está, pronto, acabou tudo. E esse é um grande sinal de pergunta. Não podemos provar quantos registratários estão utilizando suas antigas senhas para o manejo das suas registrações de nomes de domínio, então devemos estar bem conscientes do que estão fazendo.

Aqui está o de fast flux. Fast flux é uma técnica que utilizam os criminosos para passar o endereço de IP para outra de forma

rápida, para que então os profissionais de mitigação de risco ou autoridade de aplicação da lei, não consigam encontra-los.

Podem definir dentro de seus artigos, dentro do TTL, o TTL é o tempo de vida útil. O TTL é onde a direção de IP que está associada a um website seja válida. Depois os resolutores recursivos não vão poder conseguir consulta, ou fazer consultas novamente. E quando o façam vão dar um endereço de IP diferente.

Então quando vemos TTLs muitos curtos, recentemente 2 minutos, 4 minutos, há alguma coisa aí que o registro deveria olhar desconfiado. Aqui a análise é que os CDNs longos tenham sua própria operação para dar estabilidade e tudo que tenha a ver com motivos técnicos para usar TTLs, porque se a pessoa é um pesquisador, e sabe quais são os TTLs que utilizam por esta rede que pode ser muito importante. Agora se tem um domínio e um TTL corta vinculado com uma nova infraestrutura que não foi vista associada antes, e que está associada a spam, esse é um sinal de alerta. E, em geral, os investigadores da rede costumam bloquear tudo que tem a ver com a investigação dessa infraestrutura para proteção.

O duplo fast flux que acontece quando somos autoridade, pesquisamos uma infraestrutura de delinquentes que estão utilizando fast flux, vocês podem ver que o conteúdo está nesse

servidor, nesse país, minutos depois o conteúdo já não está aqui, mas em outro servidor ou outro país. Depois passa para outro país, para outro servidor. 2 minutos depois o conteúdo passa para outro servidor, quarta, quinto país. Como as autoridades lidam com isso? É muito difícil. O duplo fast flux é uma técnica que se viu em uma nuvem muito grande. Como posso dize, no servidor de nuvem de delinquentes chamado de Avalanche. Dentro de Avalanche os delinquentes fizeram um duplo fast flux. Ou seja, mudaram o nome dos servidores com muita velocidade. Então se queria fazer uma consulta com carlos agora, agora estaria fazendo nesse carlos.oquefor, em 2 minutos faria outra consulta e poderia ser nesse servidor, mas em 2 minutos fazia .camera.yahoo, a cada 2 minutos mudavam o nome do servidor. Quer dizer que a cada 2 ou 3 minutos mudavam o nome de servidor IP. É o duplo de complicação, mas os bons pesquisadores conseguiram encontra-lo, e agora graças a Deus os delinquentes já estão no cárcere, ou na cadeira, não sei.

Também falei sobre o DNS como um canal de filtrações coberto. Esse é um tipo moderno não só de filtração, mas também basicamente para o controle real do módulo do malware que se vê afetado dos dispositivos. Então através do DNS os delinquentes dão instruções aos dispositivos. Os delinquentes podem achar esse software malicioso dentro dos dispositivos. Podem injetar esse software malicioso através do DNS. E é uma dor de cabeça.

Como disse antes, o porto 53 usado para comunicações de DNS não se pode bloquear. Então o administrador tem que ter boas técnicas para bloquear essas coisas. E há técnicas que podem ser usadas, não posso falar disso agora senão seria uma sessão de 3 horas, mas cada vez tem que decidir quais técnicas aplicar.

Isso já vimos, a questão dos exemplo, dos software maliciosos, entre outras coisas, esse é outro Feederbot. Aqui podem ver então como existe uma instrução para resposta TXT do DNS. Aqui o delinquente configurou o servidor do DNS para que dê uma resposta a consulta recebida, porque a consulta figurou um registro TXT e, em realidade, aí se levam instruções para comprometer o dispositivo da consulta. Essas instruções podem ser qualquer coisa. Podem ser ataque do alvo, ao tráfego dessa forma, o que for.

Vamos ver então como evolui todo esse panorama das ameaças ao DNS. Bom, falávamos do DDoS como um serviço, não sei se vocês se lembram do MRI, alguém se lembra, que foi uma situação muito má. Mas em realidade como posso explicar isso?

Havia uma associação entre os fornecedores do que é chamado de serviços stresser e houve um ataque com esse botnet.

O que é um booter ou stresser? É um website onde alguém estabelece em algum lugar, e diz que vendem a capacidade de fazer provas para ver se seus servidores são flexíveis, e pagam o

seu dinheiro, dizem que vendem e dizem que vão mandar esse tráfego durante esse tempo para verificar a infraestrutura, para ver se é inflexível ou pode suportar um ataque.

A questão é que esses serviços stresser ou booter são vendidos a qualquer um, então operam na infraestrutura que vão operar ou não. Em outras palavras, em realidade são serviços que se alugam, e não é difícil acha-los, porque aparecem online, aparecem facilmente entre os provedores que são oferecidos, e a questão é que alguns aceitam o crédito, o cartão de crédito para pagamento, outros não, e o único que tem que fazer é pagar, e dar informação ao alvo que querem experimentar, porque obviamente querem ver se a rede é flexível.

E isso não está certo, fazem através de diferentes meios. 1 é o que são as bandas operacionais, já estivemos falando de fast flux, do duplo fast flux. Eu mencionei Avalanche, falaremos depois dele. Mas é um caso muito particular, depois veremos porque. A Internet das Coisas, não queria mencionar a palavra que está entre de e as coisas, mas a palavra que está ali não é nada mal, e é vulnerável.

Então as coisas podem sair mal. Pensem no ataque, acho que foi contra Brian Krebs em outubro de 2016, ou setembro. E frente ao OVH, que é um reigstrador realmente de muitos serviços de

hosting na França. Eles puderam detectar que o ataque vinha de algo que tinha cerca de 146.000 câmeras de vídeo.

Então a botnet podia enviar 1.5 terabytes de dados. Que é algo que não se tinha visto, porque essa quantidade de dados, em verdade, eu não posso nem imaginar na minha cabeça. Mas tinha que medir 1.1 terabytes em tráfego direto que chegava. E era de câmera de vídeo, não era uma coisa nova, mas é algo que vale a pena mencionar. O DNS foi um dos vetores utilizados nesse ataque, não o único, mas um deles.

E depois temos WannaCry que, por enquanto, vou deixar de lado.

Avalanche foi um serviço de delinquência na nuvem. Imagine que para um website gera uma conta, se registram, entram, escolhem o tipo de campanha que querem fazer, e o que fez esse pessoal foi fazer tudo por vocês. O único que você tinha que fazer era pagar algumas coisa, eles faziam todo o resto. Davam também o software malicioso, eles infectaram os clientes por vocês, faziam comando controle em nome de vocês, faziam rastreamento, um hosting para os sites distribuição dos softwares maliciosos. Foi o seguinte nível de sofisticação, porque davam serviços criminais, criminosos.

Avalanche tinha muito registro de DGA em domínios gerados por um algoritmo. Então quando perceberam as autoridades de aplicação da lei se aproximaram da ICANN, e isso se chama um

pedido expedido, e depois disso tiraram 832.000 nomes dos delinquentes. Graças a toda cooperação existente nessa altura, das autoridades de aplicação da lei do setor privado os delinquentes perderam o controle de seus rastros, está ali mas não podem tocar, não podem controlar, e realmente se sentem bem quando essas coisas acontecem. Sentimos alegria.

Essas são algumas das cadeias de caracteres criadas pela Avalanche, pela botnet para o comando de controle, e embora tenhamos esses 832.000 que estavam criados por baixo de todos esses TLDs, tanto o ccTLDs quanto gTLDs. Porque como disse, os delinquentes abusam de quem for, não se importam em nada.

E há mais alguma coisa. Alguns delinquentes, em alguns lugares do mundo, vão gerar um software malicioso para que não ataquem seus endereços de IP dentro da sua jurisdição, porque uma vez que as autoridades os persigam, isso seria ruim. Então o que fazem é pular o que são seus espaços de endereços IP.

O tema é que não podem deixar o país, então são prisioneiros de si próprios dentro das suas próprias fronteiras. É bom que fiquem ali, mas prejudica o resto do mundo. Esses são os resultados do Avalanche e do que aconteceu, devido ao conteúdo que deu a Europol e o FBI. Podemos falar desse caso em toda uma apresentação, só apresento cifras e resultados. Vejam, está na tela se querem ver os resultados, 64 TLDs, 84.000 domínios em 30 e

tantos países. E obviamente também recuperação para as vítimas e isso foi feito em grande escala. E foi algo muito bom, realmente foi um grande golpe.

O WannaCry foi algo estranho desde a perspectiva do DNS. Porque foi interessante a diferença do que se vê habitualmente no que tem a ver com tipos de software maliciosos que podem ver que tem comando de controle, no caso de WannaCry, se deu através de diferentes nomes de domínio .onion, não sei se definiu como especial, porque não podia estar nunca na raiz. A ICANN ia ter que ter a ver com esse .onion, não havia forma de tirar a infraestrutura do controle associado ao WannaCry.

Então esse pesquisador britânico Hutchins estava analisando código. Então teve ume exemplo de WannaCry, uma cadeia de caracteres que estava dentro do software malicioso. Procurou, não estava registrado. Registrou e começou a espalhar esse software malicioso por acaso. Não tinha ideia do que iria acontecer. Mas com esse nome de domínio começou a espalhar esse software malicioso agora.

O motivo está aqui. Se é ramsomware não se pode conectar com o controle, então se pode fazer analise. Estava ali infelizmente. Então o WannaCry começou a sair. Os delinquentes por trás de WannaCry tentaram registrar uma segunda cadeira de caracteres,

mas foi descoberto rapidamente. Então foi possível deter a disseminação e tiveram que sair.

O abuso de DNS é um tema controverso na ICANN. Há diferentes pontos de vista. Alguns dizem que tem a ver com a segurança, com os organismos encarregados da aplicação da lei, também tem a ver com exatidão do WHOIS, como se opera, como vai ser a aparência do WHOIS depois de 25 de maio, quando começa a ter vigência o GDPR. Também a preocupação que tem a ver com o tempo para resposta. Quando se reage a um relatório de abuso que se apresenta. Há diferentes tipos de preocupações a respeito.

Por outra parte, que é o lado em que nós como organização também temos que ouvir, esta a preocupação de que a ICANN não deve sair do seu mandato, do seu alcance, ou seja, que seu conteúdo ICANN não tem nada a ver com isso. Isso se traduz em que os contratos da ICANN não incluem disposições que falam de tirar um conteúdo que tem a ver com questões extras.

Isso tem a ver com a comunidade, e não com a organização, e são vocês da comunidade que tem a que falar desse tema. Então nós não podemos participar nessas deliberações, embora possamos facilita-las.

É importante o trabalho que faz o grupo de segurança pública, que é onde se hospedam as autoridades de aplicação da lei, onde está dentro da estrutura da ICANN tudo que tem a ver com os

comitês que se encarregam dessas questões, antes do PSWG, antes de que existisse a comunidade das autoridades de aplicação da lei, não tinham encontrado um lugar, acho que até a reunião de Beijing, quando Laureen Kapin dos Estados Unidos, como diretor executivo nessa altura, decidiram considerar ter um lugar formal para os mecanismos de aplicação da lei dentro da ICANN, e ali disseram a comunidade "bom, tragam uma proposta". Isso fizeram, e essa proposta é o que hoje conhecemos como PSWG, que é o grupo de trabalho, subgrupo dentro do comitê assessor governamental.

Ali residem o propósito do PSWG, assessoramento ao GAC e a comunidade da ICANN no seu conjunto sobre um dos temas, ou esqueci onde se concentra o abuso do DNS, os nomes de domínios são usados para fins maliciosos para provocar prejuízo, e tudo isso vai ter implicações sobre a informação do WHOIS, que está disponível para investigação, e as buscas também, a tradução de endereço de redes de grau de operador CGN, essa é uma técnica que algumas ISPs preferem não migrar para IPv6, por exemplo.

Em lugar de ter que fazer essa migração IPv6 gera redes de áreas locais muito grandes, e ali colocam os endereços de IP que só tinham que estar na internet pública que nós veríamos, se estivéssemos analisando tráfego e endereços que só tem que existir em redes privadas, que nunca deveriam ver se na internet pública. E essa é a situação na sua companhia, em suas casas,

seus dispositivos têm alocados esses endereços IPs privados. Os ISPs alocam esses endereços privados aos clientes, embora sejam 500, 10.000, 50.000, geram o nível de redes privadas, são lans.

São redes de área local com um só endereços IP público. Isso complica, porque quando batem na porta de uma casa para pegar documentos, citação, ou ISP para ter informação sobre o usuário que enviou tráfego desse endereço de IP nessa data e nesse horário, o ISP vai dizer “não sei, são 10.000 usuários que utilizam esse endereço público de IP.” E em muitos países não existe obrigação, ou talvez existe obrigação mas não é aplicada com respeito a aplicação e ao armazenamento de diferentes redes de formação, inicio da sessão, finalização da sessão, e não se guarda ali a informação e o ISP não tem informação dessa passagem. Isso foi discutido no passado, e o fast flux é a técnica utilizada pelos influentes.

Esse são 2 exemplos muito simples. De maneira alguma são exaustivos ou receptivos, são dispositivos contratuais dentro do contexto da ICANN na rede mais ampla de contratos que tem a ICANN. Pode haver muito mais. Poderíamos ter uma conversa de uma hora para falar do anti abuso do ponto de vista contratual dentro da própria ICANN. Posso mencionar que os registros tem obrigação de mencionar as suas zonas para ver se há segurança e tem obrigação de analisar os domínios que existem dentro deles. Se eu fosse o TLD de .carlos ele ia buscar todos os nomes de

domínios ali, e ver quais são as diferentes formas para a situação de comando de controle deveria informar essas métricas e estatísticas à ICANN. Essa é a obrigação do lado dos registros.

Se eu não estou enganado eu acho que os registros também tem que proporcionar a informação de abuso do ponto do contato. De parte dos registradores, há uma parte de maior especificidade, e essas disposições mais específicas estão aí nesse acordo, que se chama RAA, que é o acordo de reabilitação de registradores. Essas disposições mais específicas foram incluídas como resultado das recomendações dos organismos de aplicação da lei, que foram apresentadas pelo que agora é o PSWG, mas na época apenas era a comunidade das autoridades de aplicação da lei. Isso foi na reunião de 2012 em Costa Rica. Eu acho que eles apresentaram essas 12 recomendações, e isso fez com que a diretoria iniciasse as negociações com os registradores. Essas negociações levaram alguns meses, e resultaram no RAA de 2013 com algumas cláusulas um pouco mais específicas sobre medidas anti abuso.

Algumas têm a ver com questões que ainda precisam de mais estudo. A comunidade gostaria de ver exposições mais estritas, mas naquela época os órgãos de aplicação da lei estavam de acordo com esse texto, que foi combinado com a organização da ICANN e os grupos de parte interessadas, ou registradores.

Então rapidamente falando desse ponto, aqui se inclui que os registradores têm que tomar ações razoáveis e rápidas para investigar e responder apropriadamente qualquer relatório de abuso e força de abuso. Também tem que implicar os processos para bom acompanhamento, esses relatórios, e também tem outra obrigação que é a de dar o ponto de contato para abuso. Essa informação tem que estar publicada no website, se não estou enganado, ou nos dados do WHOIS. Eu acho que nos dados do WHOIS também tem que publicar os seus progressos websites.

Eu acho que tem que estar ali, mas não tenho certeza. Há uma disposição interessante ali, que é específica para alterar a aplicação da lei como organismo desse tipo também uma jurisdição do registrador envia um relatório de abuso desse registrados, mas lembrem que isso tem que estar dentro da própria jurisdição. O registrador tem que dar uma resposta física dentro de 24 horas. Essa resposta tem que ser dada por uma pessoa, e não de forma automática. Essa resposta não tem que ser “suspendemos o domínio”, pode ser “sim, recebemos ou avisamos que recebemos o aviso, e a pessoa que dar essa resposta, segundo este acordo, tem que ser alguém que basicamente possa decidir o que vai acontecer com esse relatório de abuso. Se deve ser suspenso ou não esse nome de domínio.

Há algumas jurisdições na qual essa cláusula é muito útil, há muitos registradores que operam naquela mesma jurisdição, mas há outras jurisdições onde há poucos registradores, ou nenhum.

Então a eficácia aos efeitos da aplicação dessa cláusula varia segundo a jurisdição da qual se trate. Depois os prestadores de serviço de privacidade e representação e proxy, que utilizam registratários para ter alguém no seu local, como informação, o WHOIS, ao invés deles próprios, se eu não quero ter o meu nome ou o meu endereço ali publica da utilizo um fornecedor de serviço de privacidade e registração, isso é controlado pelos registradores, e também tem que dar sua informação do serviço de abuso.

Eu acho que isso é tudo, esses são os temas que eu queria falar com os senhores. O abuso do DNS parece ser um tema de um ponto de vista que quando vemos um nome de domínio que se utiliza para o comando do controle de uma botnet, claramente isso é abuso, mas quando vemos podemos fazer toda a análise técnica, e não há forma de ir contra a evidência técnica que se apresenta ali, porque está ali. Mas depois há outras situações ou casos que se tornam, mas é um tema que está sempre a mesa para que seja discutido de forma contínua para que a comunidade continue expandindo o conhecimento sobre esses temas. Mas no começo eu falei, eu sou diretor de segurança ou de relacionamento de segurança e estabilidade e flexibilidade com a

equipe encarregada desses aspectos, estou no escritório de CTO, trabalhamos com as autoridades de aplicação da lei e fazemos muitas coisas.

Tentamos de nos vincular com autoridades da ICANN, queremos que eles entendam todas as discussões que levamos aqui. Há algumas semanas, um representante da indústria de nomes de domínio, participou de uma conferência de segurança pelo nosso convite, é um grupo de trabalho de Jonathan Frakes, que é diretor executivo da associação de nomes de domínio, e houve interações muito positivas nesse encontro, e essa é uma das coisas que fazemos. Nos relacionamos, tratamos de trazer aquelas pessoas que tradicionalmente foram vista como lados opostos, para que cheguem a um terreno em comum. Para que entendam que se pode construir alguma coisa com base nesse terreno em comum.

Também trabalhamos com os organismos de proteção, um dos nossos escritórios da ICANN queria manter uma das funções é manter a função e a flexibilidade do nome de domínio. Isso significa que as autoridades de aplicação da lei tem que entender o que significa quando estão fazendo uma investigação de uma situação do caso de botnet, ou de questões criminosas, e nós ajudamos para que eles entendam, e se mantenham afastados do sistema sem interferir. Embora utilizamos outros termos para definir.

Se tem alguma pergunta, por favor, sintam-se em liberdade.

CATHY PETERSEN: Digam seu nome e a origem se tem alguma pergunta. Obrigada.

MARSY SURMO: Eu sou da Índia, e eu quero fazer uma pergunta e um comentário. A ICANN preparou algumas normas de segurança básica para as operações de internet, poderiam ser aplicadas, embora estejam essas normas continuam existindo ataques, e sempre se pode fazer uma análise depois de feito o fato. O que podemos fazer para poder prever e que não chegue a afetar a função do DNS.

CARLOS ALVAREZ: Eu sugiro que veja os documentos publicados no DNS.org, que é da comunidade dos operadores de DNS, onde ali podem ter alguns elementos de segurança para o DNS. Procurem M3AAWG DNS, essa será a abreviação. Faz um ano e meio, atualizaram o que se conhece como nome de, agora não lembro, se procuram com esta sigla de pós ameaças ao DNS vão encontrar e aí vão encontrar a informação. Essas são as comunidades do grupo que eu acho que trabalharam em documentos e normas como aqui você menciona.

MARSY SURMO: Eu quero algum tipo de orientação de critério geral para estar seguro de que se apliquem suas normas mínimas.

CARLOS ALVAREZ: Qualquer um pode operar um servidor DNS no mundo. Não há forma de aplicar essas normas, é impossível prevenir, não é regra, nada vinculante. Eles podem fazer da forma voluntária, do jeito deles. O que não facilita as coisas claro.

Agora com respeito ao comentário que o senhor faz, se falamos do elemento voluntário, se há normas e formas de fazer as coisas já definidas pela comunidade técnica de 1997, a arbitragem dos endereços e IPv4, por exemplo, se vocês vêm o BCP e outras práticas, vão ver que existem há anos. Há práticas que não foram tão amplamente como o pessoal quer, apesar de estar em vigor há muito tempo, porque são de cumprimento voluntário.

Alguma outra pergunta, por favor?

Seu nome, por favor.

HARU AL HASSAN: Eu sou Haru Al Hassan da Nigéria. Nos países em desenvolvimento temos um desafio, como treinamos os organismos de aplicação da lei para estar a altura desses criminosos? Porque o senhor demonstrou muitas formas como

se pode envenenar e atacar o DNS de diferentes formas. Então como treinamos os funcionários da aplicação da lei para poder estar a altura desses criminosos?

CARLOS ALVAREZ: Eu acho que um caminho adequado para isso seria entrar em contato com o pessoal de relacionamento da ICANN na África, eu não sei se o senhor já os conheceu aqui, e manifestar a sua preocupação com a pessoa que está a cargo dessas relações. Essa pessoa com nosso equipe desse SSR vai coordenar, e vai fazer com que os organismos de aplicação da lei participem em uma capacitação que nós damos sobre abuso do DNS.

Eu sugiro que procure essa pessoa Pierre, que a preocupação que o senhor tem é muito válida.

BRENT CAREY: Eu sou Brent Carey. Semana passada eu cheguei de Ottawa e vi que havia uma cadeia de caracteres com nome de domínio e havia um abuso de infraestrutura de conteúdo, e tudo isso está surgindo cada vez mais, então o que podemos fazer a respeito.

CARLOS ALVAREZ: Eu não sei. Eu não tenho essa resposta, mas eu sei que organizaram esse fórum em Ottawa, alguns colegas estiveram ali.

BRENT CAREY: Porque houve uma ausência dos organismos de aplicação da lei ali.

CARLOS ALVAREZ: Está bem, tomo nota. Talvez teremos que falar sobre essa questão em particular.

Mais alguma pergunta?

PESSOA NÃO IDENTIFICADA: Nós não temos um mecanismo sólido para cumprir com o GDPR e com o WHOIS, e também não temos controle sobre esses temos de segurança, então vai ser muito difícil no futuro, pelo menos isso parece, né?

CARLOS ALVAREZ: O que vai ser difícil?

PESSOA NÃO IDENTIFICADA: Nós falamos que não tínhamos um WHOIS autentico, então agora vamos ver o GDPR.

CARLOS ALVAREZ: Sim.

PESSOA NÃO IDENTIFICADA: Não há controle sobre esses pontos. Os operadores falaram todos juntos, peçam desculpas, não sabem para onde vão.

CARLOS ALVAREZ: A minha sugestão é que participem em todas essas deliberações, que participe e faça os seus comentários e tudo que tem a ver sobre as videconferências. Então eu peço que o senhor participe, porque essa é a forma na qual poderão escutar a sua sugestão, e de fato se escuta, não é uma coisa retórica, são escutados de verdade. Se os senhores têm preocupações e essas são válidas.

Estas são algumas sessões, não são as únicas que são importantes, embora tenham relação com o abuso de DNS, que estão aqui na tela. Se vêm, ontem 11:30, se podem voltar no tempo, poderiam ter visto o que o relatório do PSWG, amanhã, terça-feira, temos outra reunião do PSWG com o GAC. Eu peço que participem do GDPR. Nos encontram nesse cruzamento de caminhos entre as diferentes coisas. Ambas as reuniões serão bem importantes, e também veremos o que faz a indústria de

nomes de domínio com sua própria iniciativa para ver o que estão fazendo.

São coisas interessantes, depois DAAR é uma ferramenta que está se desenvolvendo, e que dá informação sobre o que são as más registrações, ou como podemos acrescentar isso e evitar trabalhos duplicados. E isso é muito interessante, eu estaria interessado em que participem e que se divirtam.

Obrigado a todos pela presença.

CATHY PETERSEN: Para lembrar, as apresentações já estão no cronograma público, depois também serão colocadas as transcrições. Tudo estará no cronograma público em poucos dias, então qualquer coisa podem se remeter ali e ver tudo novamente.

Agora vamos ter a seguinte sessão de como funciona as 15:30, e não 15:15 como disse aqui, que é como funciona a rede da internet. Um pouco mais tarde que o previsto. E nesse trabalho sobre a sessão, vamos falar do IPv4 e IPv6, sobre ambos os protocolos. Então eu peço que tomem um café e voltem 15:30. Obrigado.