SAN JUAN – Atualização sobre a implantação da KSK
Quarta-feira, 14 de março de 2018 – 16h15 to 16h45 AST
ICANN61 | San Juan, Porto Rico

PESSOA NÃO IDENTIFICADA: Vamos começar daqui a pouco. Por favor, vocês podem projetar a apresentação aqui na tela?

Vamos começar daqui a 30 segundos.

Oi a todos. Essa é a sessão de atualização da troca da KSK. Eu espero que tenham pessoas aqui que não tenham já me visto falando sobre isso. Vou recapitular do que temos feito hoje. Essa troca foi programada para 11 de setembro de 2017. Decidimos adiar isso, e a Verisign analisou o RFC 8145, usaram o relatório da ancora de confiança enviadas para os servidores [inaudível] de raiz, e não houve um novo retorno a KSK. Esses 7-8% teve algo que ficou errado, e essa análise com o tráfego de diferentes servidores raiz foi feita. Encontramos uns resultados, dependendo de como vemos resultados. Vemos que as percentagens são um pouco diferentes, mas não entendemos porque esses resolvedores estavam informando a antiga chave.

Então tentamos determinar porque tinha acontecido isso. Estavam utilizando a antiga. Então fizemos uma lista em

setembro de 2017, 100 resolvedores que tinham informado a antiga chave. Ver qual aprova, e rastreamos os operadores com base apenas no IP. Os operadores de só 20% de endereços seriam então contatados.

Também houve um problema com o RFC 8145. Sabíamos que havia problemas com o sinal, como esses resolvedores estão utilizando apenas o 2010. Não havia uma única causa, esse era o problema. Se tivéssemos tido 1 ou 2 causas teria sido bem mais fácil, teríamos falando aos fornecedores de como reparar isso, mas não era bem assim. Então não tínhamos uma maneira de como continuar. Então pedimos à comunidade que opinasse. Fizemos um período de comentários públicos pedindo por opiniões através de uma lista de email. O KSK rollover. E eu sugiro aqui quem não estiver nesta lista de emails, por favor, inscreva-se, porque é muito útil.

Quanto a discussão dos resultados foram um acordo em que não havia aqui uma medição acurada da quantidade dos usuários que seriam afetados pela troca do KSK raiz, e sugeriram que seria bom fazer boas medições para as futuras trocas de KSK. Havia uma série de usuários. Ali seria uma boa maneira de medir isso. Não é o que o RFC 8145 estava determinando, mas era uma boa ideia. Então estávamos esperando pelo Sentinela, que é preliminar da APNIC, que são medições com base nos usuários. Não temos isso agora, e o

consenso do grupo é que a ICANN org deveria fazer a troca da KSK de forma pontual, e oportuna.

E com base no feedback em primeiro de fevereiro nós publicamos um plano preliminar. E estava formado a decisão de adiar por um ano a troca para obtermos critérios, por enquanto não tínhamos critérios específicos mensuráveis, que tinham surgido durante a discussão com a comunidade. Continuamos publicando mais observações para os dados de assinatura de âncora de raiz. E isso faria com que isso tudo fosse mais útil, mais seguro. E algo importante é que nós tivemos esse comentário público aberto. Esse plano é apenas um plano preliminar. Ele vai ficar encerrado em 2 de abril de 2018. Aqui temos o URL do site para entrar no comentário público. E se nós terminarmos o plano, completarmos o plano da maneira que está aqui nesse cronograma, teríamos 2 de abril final do comentário público, meados de abril começamos a publicar o relatório, depois a revisão do plano, se for preciso a publicação.

Bom, as reuniões da ICANN são feitas 6 vezes ao ano, 3 presenciais e 3 não. Temos uma oficina. Então a próxima vai ser em meados de maio. É uma oficina e nessa oficina vamos solicitar que a diretoria solicite a RSSAC, comente o plano antes de primeiro de agosto. Vamos ter uma sessão no Panamá, depois também em junho. E já em primeiro de agosto esperamos ter recebido feedback do RSSAC, revisar o plano, e se

tudo isso funcionar bem, em meados de agosto teremos publicado esse plano final, e em setembro teremos a oficina com a resolução encaminhada a ICANN org para a troca da KSK em outubro de 2018. É só isso.

Então estamos esperando pelo feedback da comunidade. Gostaríamos muito que o pessoal participasse. O resto da apresentação vamos falar sobre os sinais no RFC 8145 São relatórios de âncora de confiança. O CTO da ICANN tem acesso a RFC 8145 e seus dados de 11 servidores de raiz. São 11 ou 12. Porque agora adicionamos o H, então são 12, não são 11. A análise inicial, no final de 2017, utilizou dados backup de B, D e F. Mas temos usado um plug in excelente com o DNS cap. Com relatórios a cada 60 segundos que analisa o tráfego através de batches. Relatórios de âncoras de confiança que também ocorre através de consultas do DNS, e é muito bom. E vemos como opera aqui. Temos o exemplo de timestamp, o ID do resolvedor, os âncoras que estão configurados aqui. Para o KSK 2010, o 4F66 é para 2017.

Então com base me tudo isso nós conseguimos fazer esse gráfico aqui. Vemos como o tempo vai progredindo com cada vez mais relatórios. É um gráfico um pouco complexo. As linhas nos mostram coisas verdes, a quantidade de IPs nos relatórios de dados de âncora, vemos isso através do tempo. Vemos a linha verde com quantidade total de fontes que informam dados

de confiança. São fontes únicas por dia. São 15.000 aqui por cada dia. A vermelha ela informa só a KSK de 2010, então se dividimos a verde pela vermelha obtemos essa percentagem que é a linha preta, que são as fontes que informam só a KSK 2010. Agora estamos em 20% de resolvedores que informam a antiga KSK.

Temos cada vez mais pessoas informando, e temos a certeza que isso é resultado de um upgrade do unbound, que foi lançado em janeiro de 2008, e essa habilitação de lançamento foi muito positiva. Foi um batch de segurança, mas não há nenhuma queda na KSK 2010 depois de 30 dias.

Então se alguém operar esse unbound, e não uma âncora tool. Então se alguém faz o unbound, eles vão atualizar de imediato a KSK 2010 e 2017. Agora então ainda estamos com a antiga chave, e depois de 30 dias podemos repetir o processo, e podemos incluir também a 2017, mas de fato isso não está acontecendo, por que? Porque temos essas máquinas virtuais, ou containers efêmeros. Talvez essa seja a causa.

Então temos os relatórios de 2010 que funcionam por alguns dias, horas, depois entram em pausa, e depois reiniciam, e só informando o KSK 2010. Devemos continuar analisando. Acho que estivemos preparando esses slides para essa reunião que estão aqui. Também temos os endereços de IP com diferentes

tipos de relatórios, tipos unboud. Temos IPs que não estão fazendo isso, e talvez seja por esses efêmeros que sobem e descem. Estamos tentando determinar porque, e aqui temos gráficos para as redes individuais. São para todos os servidores raiz. São 11. Tínhamos 11 quando fizemos isso, com diferentes servidores, diferentes períodos, e se observarmos todos eles são bastante parecidos. Exceto que a raiz é um pouco diferente, a raiz J é um pouco diferente. O que é interessante aqui é a conduta que observamos em meados de junho, e o gráfico mostra endereços IP a cada dia, e aqui vemos nesse dia único. Quantas fontes únicas informam dados de âncora de confiança adicionadas por dia. Quantas são adicionadas por dia? Temos 100 a cada dia. E depois de janeiro isso foi aumentando. Entre 15.000, e 16.000.

Também seria muito bom ver um gráfico que mostrasse essas fontes cumulativas. Veríamos como começa um número bem baixo, depois vai aumentando. Temos agora um que é 730.000 endereços IP. Uma combinação de endereços, e IPv4 e IPv6. Que informaram que só tinham KSK 2010. E se observamos números cumulativos vemos que há um aumento de 35%. E isso só informando KSK 2010.

Eu decidi ver o barra 24. O formato desse gráfico é muito diferente. Há um pico em janeiro, e se nós vermos o gráfico acumulado há muito barra 24. Veja em verde, chega a 35.000 em

média. São 2 IPs por barra 24. Eu esperava que esse número fosse menor. E que seriam blocos inteiros de endereços que pudéssemos investigar. E uma boa hipótese seria que talvez seriam máquinas efêmeras apenas.

São muitos endereços então. O que é interessante é que o número total de endereços que informam KSK 2010, e 2017, é maior do que o número total de IPs únicos, o que significa que há fontes que relataram KSK 2010. E depois relataram KSK 2017. Não necessariamente nessa ordem, mas relataram duas vezes.

E uma razão disso, imaginem que uma fonte ela adota KSK 2010, e mais tarde KSK 2017. Essa é uma das razões disso, mas não é a única. Que essa máquina fez um upgrade, e tem um novo KSK. Mas como que esses três quartos de milhão de IP, só poucos relataram isso? Essas 1.559 fizeram essa atualização.

Há um problema com esse sinal. Se vê um relato de uma fonte de IP, não se tem garantia que é essa máquina, outra pessoa está fazendo, está encaminhando que vai depois encaminhar para o servidor raiz, e aí que vemos uma única fonte relatando o KSK 2010 e 2017.

Há uma implementação que relatou esses dados, mesmo invalidados. Se fosse KSK 2010, estava sendo usado como parte das configuração. Estava sendo usado, mas não utilizou. Esses gráficos estão sendo atualizados semanalmente nesse endereço

aqui na tela. Eu comecei a fazer então o detalhamento dos dados. São os 250.000 que relataram o KSK, não são todos aqui. São os números de fontes por sistema autônomo, e fazemos a busca reversa. E se vê que a maior parte dos IPs. Desculpem, KSK 2010. Esses são informes de sistemas autônomos.

O que isso significa? Isso deve ser analisado novamente para ver só o KSK 2010, para tentar descobrir o que está acontecendo com as ASNs que tem o maior número de resolvedores informando o KSK 2010. Então distribuímos uma lista de IPs que informa apenas a KSK 2010. E o objetivo é duplo. Esses sistemas precisam ser atualizados, ou upgraded. E se nós vermos, por exemplo, o melhor, um dos melhores resultados seria ver que de fato nesse endereço há várias máquinas efêmeras. Seria um achado positivo. Esse slide está desatualizado. Eu tenho autorização para tornar essa lista disponível. E essa lista vai ser então organizada por ASN, e você vai poder clicar e vai poder ver os detalhes das ASNs. E vai ajudar os operadores a ver o que está acontecendo. E nós vamos contatar os operadores, especialmente os que têm maior informe de KSK 2010, para ver o que está acontecendo.

Então quais são as próximas etapas? É continuar a investigar. Nós temos que continuar utilizando esses dados do RFC 8145. Eu não acho excelente, mas é o que está disponível. Então, se não há variação, isso sim é um achado positivo. Como eu disse,

vamos contatar as ASNs que informam apenas o KSK 2010, e vamos estimular outros a continuar a pesquisar, e vamos continuar a anunciar essa troca do KSK, e ouvir a comunidade também. Aqui novamente eu mostro o link para o site. Eu gostaria muito que vocês contribuíssem. Muito obrigado por me ouvirem. Temos ainda um tempinho antes do próximo evento. Se tiverem alguma pergunta.

HOWARD BENN: É Howard Benn da Samsung Electronics. Sobre aquele slide sobre todos os operadores. Esse aí. Então eu acho que, provavelmente, é o trabalho do LTE. São máquinas virtuais e nunca vão chegar ao limite de 30 dias. Seria muito interessante saber que na verdade há um grande número de operadores móveis. E tem esse mesmo problema. E eu posso então dar informações de contato para que vocês possam falar com esses operadores de celular.

MARK: Mark [inaudível]. Estou falando a título pessoal. Você poderia voltar para o slide número 4? Esse aí. Eu estou vendo na parte de baixo do slide de resultados e discussão.

Em primeiro lugar diz que nós não sabemos qual é o efeito disso sobre a internet. E o terceiro item diz para fazer isso de qualquer maneira. Eu estou lendo isso errado?

PESSOA NÃO IDENTIFICADA: Bom, seria uma interpretação do copo meio cheio, ou meio vazio. Bom, eu vou dar a resposta séria. É que é um problema difícil de decidir o que fazer. Quando chegamos ao último outono decidimos que precisávamos envolver a comunidade, e da contribuição da comunidade. Então esse resumo foi o que a comunidade nos disse. As pessoas que trabalharam com KSK defendem o DNSSEC, capital pessoal, e quem investiu no DNSSEC quer que essa troca ocorra. E é por isso que o comentário público é tão importante para que isso seja exposto para um número maior de pessoas, para ter uma interpretação diferente.

MARK: Muito obrigado pela explicação, mas eu continuo com a perspectiva do copo meio vazio. Então eu estou aqui defendendo o DNSSEC, mas eu não consigo entender, e eu vou falar individualmente. 1 e 3 me parece meio estranho que alguém proponha seriamente fazer uma mudança na raiz que não saiba qual é o efeito disso. Eu estou de acordo com vocês. Eu confio na sua análise que há uma má qualidade da

sinalização. E é a única informação de diagnóstico que nós temos. E a situação só fica pior. Bom, isso é minha interpretação da situação. Então eu acho esse slide, e os outros que vêm depois, eles colocam muito bem o ponto. Mas esse item, esse terceiro item aí eu não conheço ninguém da comunidade técnica que diria “bom, vai lá e troca a chave” mas não sabemos qual é o resultado. Muito obrigado de qualquer forma pelo comentário.

PESSOA NÃO IDENTIFICADA: Deixa eu dar talvez uma outra interpretação. Não é minha interpretação. Estou repetindo o que ouvi. É que há uma desvantagem em não trocar a chave que é diminuir a confiança na chave. Então não há uma ameaça a segurança física das operações, a criptografia, mas de qualquer forma, se não houvesse a troca diminuiria a confiança, e talvez o que aconteça não seja muito grave, pode ser consertado rapidamente. Então se deveria trocar a chave.

MARK: Eu entendo a questão da reputação. Bom, o que nós queremos é trocar a chave, porque queremos que as pessoas tenham confiança no DNSSEC. Mas, por outro lado, se as pessoas estão imaginando ou adivinhando da forma errada, então se nós tivermos que voltar atrás, isso não foi feito ainda. E eu acho que

há um problema de reputação de qualquer forma, e coloca a ICANN em uma posição bastante difícil. Eu não estou tão convencido que a questão da reputação do DNSSEC seja tão grave como essa implementação, que tenha um efeito desconhecido em outubro.

PESSOA NÃO IDENTIFICADA: Cathy, você quer falar alguma coisa da internet?

PESSOA NÃO IDENTIFICADA: Minha pergunta é: nós verificamos na Nigéria, uma grande parte dos provedores de IPs usa DNSSEC, outros têm outro sistema de habilitação. Diferente do DNSSEC. A minha primeira pergunta é: qual é a vantagem do DNSSEC em relação a outros sistemas de validação de segurança? Há uma necessidade dos operadores migrarem para o DNSSEC?

PESSOA NÃO IDENTIFICADA: Poderia repetir a última parte da pergunta?

PESSOA NÃO IDENTIFICADA: O que eu disse é que os 3 dos provedores de rede de serviços móveis não usam o DNSSEC, usam outro sistema. Qual seria o efeito? Qual seria o impacto se eles não fizerem o KSK?

PESSOA NÃO IDENTIFICADA: Se você não usa o DNSSEC não há impacto da troca do KSK. A ICANN acha que a validação do DNSSEC é uma coisa interessante, então fazemos isso. Mas desculpe. Eu não me lembro agora da primeira parte da pergunta.

PESSOA NÃO IDENTIFICADA: Na primeira parte, qual é a vantagem dos que não usam DNSSEC para migrar para o DNSSEC?

PESSOA NÃO IDENTIFICADA: A posição da ICANN org é que se deve fazer a validação pelo DNSSEC, porque senão não há garantia de que a resposta que você recebe está respondendo a pergunta que você fez. E vindo de onde você acha que fez a pergunta. Então não há garantia criptográfica de que as respostas que você está recebendo vêm da fonte para que você perguntou, e o DNSSEC sim. Então os resolvedores se tornaram muito inteligentes para evitar ser enganados, mas é necessário validar o DNSSEC. Então sem o DNSSEC você pode sofrer spoofed.

PESSOA NÃO IDENTIFICADA: Muito obrigado.

PESSOA NÃO IDENTIFICADA: Alguma outra pergunta? Muito bem, muito obrigado por virem.