Revisão da chave de assinatura de chaves (KSK) da zona raiz

Visão geral da revisão da KSK

A ICANN está planejando revisar ou alterar uma parte do par de chaves criptográficas usadas no protocolo das Extensões de Segurança do Sistema de Nomes de Domínio (DNSSEC), conhecidas como KSK da zona raiz. Essa será a primeira alteração da KSK desde sua geração em 2010.

Trata-se de uma medida de segurança importante, da mesma forma que a mudança frequente de senhas é considerada uma prática prudente para qualquer usuário da Internet.

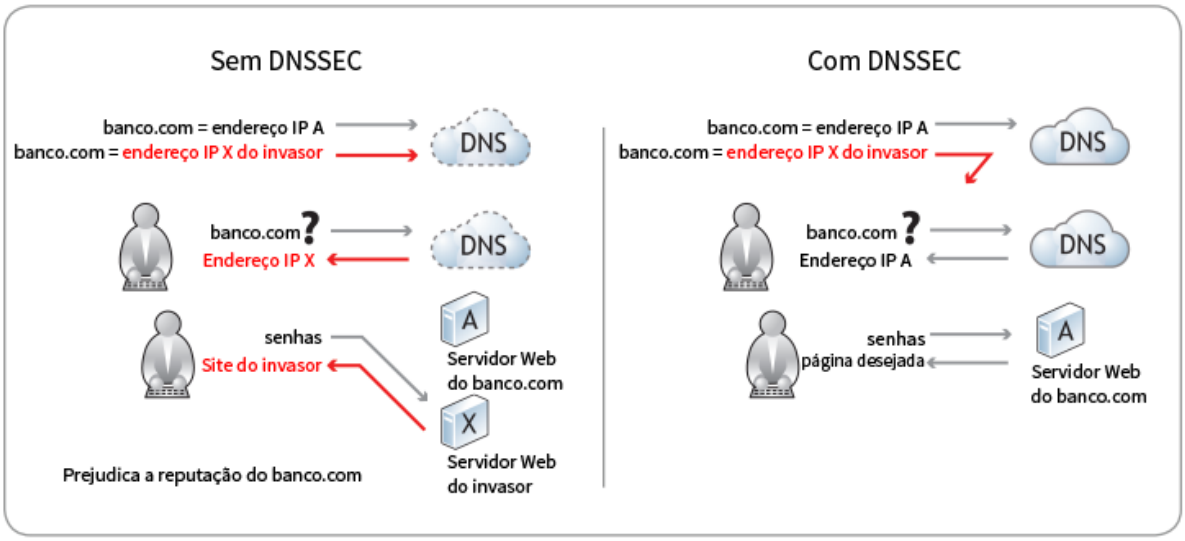
A KSK da zona raiz consiste em uma chave privada e uma pública. O componente privado é armazenado de forma segura pela ICANN, mas o componente público é amplamente distribuído e configurado em vários dispositivos, podendo chegar a um milhão. O processo de revisão da KSK tem várias etapas e basicamente envolve a geração de um novo par de chaves criptográficas e a distribuição da nova chave pública.

Os provedores de serviços de Internet, operadores de redes corporativas e outros que façam a validação de DNSSEC devem atualizar seus sistemas com a parte pública da nova KSK para garantir que seus usuários continuem acessando a Internet sem problemas.

A KSK é um componente essencial das DNSSEC, uma tecnologia de segurança que autentica a integridade das informações no sistema de nomes de domínio (DNS), que é a lista telefônica global da Internet. Esse tipo de mudança nunca ocorreu no nível da raiz, então a revisão deve ser coordenada com muito cuidado para garantir que ela não interfira com as operações normais. Por isso, a ICANN está informando as comunidades de operadores e usuários da Internet sobre as mudanças agora, antes que a revisão seja feita.

Qual é a função da KSK nas DNSSEC?

Através da validação de dados do DNS, a KSK desempenha um papel importante na proteção dos usuários da Internet contra o sequestro de nomes de domínio por pessoas mal-intencionadas, buscando ganhos financeiros ilícitos. Por exemplo, a tentativa de acessar informações bancárias pode fazer com que o usuário seja redirecionado a um site que rouba dados de identificação e senhas.



Por que a revisão da KSK é importante?

A KSK foi distribuída a todos os operadores que fazem a validação de DNSSEC. Se os resolvedores de validação que usam DNSSEC não tiverem a nova chave quando a KSK for revisada, seus usuários finais encontrarão erros e não poderão acessar a Internet.

A KSK da zona raiz é a primeira chave de uma cadeia de chaves públicas usada pelos resolvedores de validação para confirmar a autenticidade dos dados do DNS. Cada chave da cadeia confirma a validez da próxima, começando pela KSK da raiz. Se ela mudar e a configuração do resolvedor não for atualizada, a primeira chave da cadeia ficará errada, invalidando todas as outras. Dessa forma, a validação de DNSSEC falha e esse erro impede os usuários de acessar a Internet.

Quando será a revisão?

A revisão da KSK é um processo, não um evento único, e deve ser concluída em março de 2018. A ideia é que a nova chave pública seja publicada em http://data.iana.org/root-anchors/ em fevereiro de 2017 e que apareça no DNS pela primeira vez em 11 de julho de 2017.

Estas são algumas outras etapas do processo de revisão. As datas estão sujeitas a mudança devido a considerações operacionais:

- **Outubro de 2016:** geração da nova KSK
- **Fevereiro de 2017:** publicação da nova KSK no site da IANA
- **Julho de 2017:** publicação da nova KSK no DNS
- **Outubro de 2017:** uso da nova KSK para assinatura (a revisão em si)

- **Janeiro de 2018:** revogação da KSK antiga
- **Março de 2018:** destruição segura da KSK antiga e conclusão do processo de revisão

Quantas pessoas podem ser afetadas?

A estimativa é de que um a cada quatro usuários da Internet no mundo todo, ou seja, 750 milhões de pessoas, sejam afetados pela revisão da KSK. Essa cifra se baseia no número estimado de usuários da Internet que usam resolvedores de validação de DNSSEC.

Quem precisa tomar medidas?

Os desenvolvedores de software que dão suporte à validação de DNSSEC devem garantir que seus produtos sejam compatíveis com o protocolo de atualização da âncora de confiança RFC 5011. Os desenvolvedores e distribuidores de software que incluem a KSK da zona raiz em códigos ou arquivos de configuração devem usar a nova KSK, de preferência assim que possível depois de sua publicação em fevereiro de 2017.

Os operadores que usam o protocolo automático de atualização da âncora de confiança RFC 5011 devem configurar seus resolvedores habilitados por DNSSEC para atualizar automaticamente a âncora de confiança da zona raiz quando a revisão acontecer. Os operadores que atualizarem manualmente a configuração da âncora de confiança do resolvedor habilitado por DNSSEC devem fazer isso até 11 de outubro de 2017.

As pessoas que gravam, integram, distribuem ou operam softwares que façam validação de DNSSEC seguindo corretamente o protocolo automático da âncora de confiança RFC 5011 não precisam tomar medidas.

Recursos

Faça uma pergunta

Envie suas perguntas por e-mail para globalsupport@icann.org com o assunto "KSK Rollover".

Saiba mais sobre a revisão da KSK

https://www.icann.org/kskroll

Participe da conversa

Use a hashtag #KeyRoll: **https://twitter.com/icann**