Traspaso de la clave para la firma de la llave de la zona raíz (KSK)

Sinopsis del traspaso de la KSK

La ICANN está planificando traspasar, o cambiar, el par "superior" de claves criptográficas que se utiliza en el protocolo de Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC), comúnmente conocido como la KSK de la zona raíz. Ésta será la primera vez que se cambie la KSK desde que se generó inicialmente en el año 2010.

El cambio de estas claves de DNSSEC es un paso importante relativo a la seguridad, de la misma manera que el cambio periódico de contraseñas es considerado una práctica prudente por todo usuario de Internet.

La KSK de la zona raíz consiste en una clave privada y una clave pública. El componente privado es almacenado de modo seguro por la ICANN, pero el componente público es ampliamente distribuido y configurado en una gran cantidad de dispositivos, posiblemente en un número que asciende a millones. El proceso de traspaso de la KSK que consta de varios pasos básicamente implica generar un nuevo par de claves criptográficas y luego distribuir la nueva clave pública.

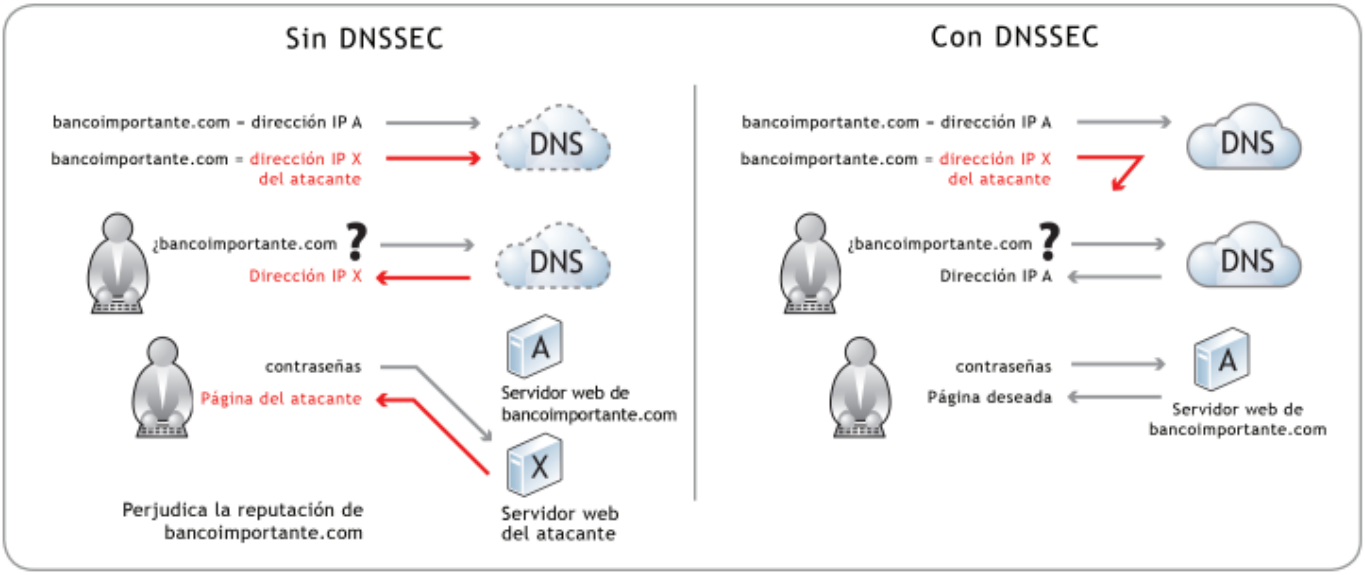
Los proveedores de servicios de Internet, operadores de redes empresariales y otros que realizan la validación de DNSSEC deben asegurarse de que sus sistemas estén actualizados con la parte pública de la nueva KSK a fin de garantizar el acceso a Internet sin inconvenientes para sus usuarios.

La KSK es un componente esencial de las DNSSEC, una tecnología de seguridad que autentica la integridad de la información dentro del Sistema de Nombres de Dominio (DNS), que constituye la guía telefónica global de Internet. Este tipo de cambio nunca se ha realizado antes a nivel de la raíz, por lo que el traspaso debe ser coordinado de manera amplia y cuidadosa a fin de garantizar que no interfiera con las operaciones normales. Por este motivo, la ICANN está informando ahora a las comunidades de usuarios y operadores de Internet sobre los cambios, antes de que se lleve a cabo el traspaso.

¿Qué rol tiene la KSK en las DNSSEC?

La KSK tiene un rol importante en proteger a los usuarios de Internet del secuestro de nombres de dominio mediante la validación de los datos del DNS. Tal como lo indica la frase, el secuestro de nombres de dominio es tomar el control de un nombre de dominio, generalmente por parte de aquellos con intenciones maliciosas que pueden desear obtener una ganancia financiera ilícita.

Por ejemplo, los intentos para acceder a información de cuentas bancarias pueden resultar en redirigir a los usuarios a un sitio que roba la identificación y las contraseñas.



Por qué es importante el traspaso de la KSK

La KSK ha sido ampliamente distribuida a todos los operadores que realizan la validación de las DNSSEC. Si los resolutores de validación que utilizan las DNSSEC no tienen la clave nueva cuando se realice el traspaso de la KSK, los usuarios finales que dependen de dichos resolutores encontrarán errores y no podrán tener acceso a Internet.

La KSK de la zona raíz es la primera clave en una cadena de claves públicas que un resolutor de validación utiliza para confirmar la autenticidad de los datos del DNS. Cada clave de la cadena garantiza la validez de la próxima clave, a partir de la KSK de la raíz al comienzo de la cadena. Si la KSK de la zona raíz se modifica y la configuración del resolutor no se actualiza, la primera clave de la cadena será incorrecta, lo que hará que toda la cadena no sea válida. Como consecuencia, la validación de las DNSSEC fallará y el error resultante impedirá que los usuarios tengan acceso a Internet.

¿Cuándo tendrá lugar el traspaso?

El traspaso de la KSK es un proceso, no un evento único, que se prevé que finalice en marzo de 2018. La clave pública nueva se ha programado tentativamente para ser publicada en http://data.iana.org/root-anchors/ en febrero de 2017 y aparecerá en el DNS por primera vez el 11 de julio de 2017.

A continuación, se muestran algunos otros hitos en el proceso de traspaso. Nótese que estas fechas están sujetas a cambio debido a consideraciones operativas:

- **Octubre de 2016:** Generación de KSK nueva
- **Febrero de 2017:** Publicación de KSK nueva en el sitio web de la IANA
- **Julio de 2017:** Publicación de KSK nueva en el DNS
- **Octubre de 2017:** Se utiliza KSK nueva para la firma (el evento de traspaso real en sí)
- **Enero de 2018:** Revocación de KSK anterior
- **Marzo de 2018:** Destrucción segura de KSK anterior y finalización del proceso de traspaso de KSK

¿Cuántas personas podrían verse afectadas?

Se estima que uno de cuatro usuarios globales de Internet o 750 millones de personas podrían verse afectados por el traspaso de la KSK. Esa cifra se basa en la cantidad estimada de usuarios de Internet que utilizan resolutores de validación de DNSSEC.

¿Quiénes necesitan realizar acciones?

Se recomienda encarecidamente que los desarrolladores de software compatibles con la validación de las DNSSEC brinden soporte al protocolo de actualización de anclaje de confianza automático RFC 5011. Los desarrolladores y distribuidores de software que incluyen la KSK de la zona raíz en archivos de configuración o código deben garantizar que la nueva KSK de la zona raíz sea utilizada, idealmente tan pronto como sea posible después de la publicación de la KSK nueva en febrero de 2017.

Los operadores que dependen del protocolo de actualización de anclaje de confianza automático RFC 5011 deben garantizar que sus resolutores activados con DNSSEC estén configurados para que actualicen automáticamente el anclaje de confianza de la zona raíz cuando se lleve a cabo el traspaso. Los operadores que actualizan manualmente la configuración de anclaje de confianza de resolutores activados con DNSSEC deben garantizar que la nueva KSK de la zona raíz esté configurada antes del 11 de octubre de 2017.

Todos aquellos que escriben, integran, distribuyen u operan software compatible con la validación de las DNSSEC que cumplen correctamente con el protocolo de anclaje de confianza automático RFC 5011 no necesitan llevar a cabo ninguna acción.

Recursos

Formule una pregunta

Para presentar una pregunta, envíe un correo electrónico a globalsupport@icann.org con la línea de asunto "Traspaso de KSK".

Conozca más sobre el traspaso de KSK

https://www.icann.org/kskroll

Participe de la conversación

Utilice el hashtag #KeyRoll: **https://twitter.com/icann**