KOBE – Taller sobre las DNSSEC (2 de 3)
Miércoles, 13 de marzo de 2019 – 10:30 a 12:00 JST
ICANN64 | Kobe, Japón

JACQUES LATOUR: Buenos días. Estamos en la segunda parte de nuestro taller. Tenemos cuatro presentaciones; las primeras dos acerca de las DNSSEC, DNS-sobre-TLS y DNS-sobre-HTTPs y luego hablaremos sobre el traspaso de la KSK.

Ahora tenemos a Warren Kumari de Google que será nuestro próximo orador.

WARREN KUMARI: Les pido disculpas por adelantado, quizás no sea muy amable de mi parte dado que estamos en un taller de las DNSSEC, pero estas DNSSEC realmente insumen mucho trabajo, ya tienen como 20 años y hay muchos otros protocolos como DNS-sobre-TLS y DNS en HTTPS. Si yo tengo estos otros protocolos, ¿realmente vale la pena hacer todo este trabajo para implementar las DNSSEC?

Bueno, muy bien. Vamos a hablar entonces acerca de esto. En primer lugar les aclaro que esta es una introducción, he simplificado algunos conceptos y en algunos casos hay simplificaciones incluso excesivas. Voy a controlar el tiempo también de mi presentación para no excederme.

En primer lugar tengo que hablar acerca de la protección, de la confidencialidad y de la integridad, que son dos cosas diferentes.

Me piden que me acerque al micrófono, pero yo soy un poco bajito y no llego. Bueno, ahí va.

Entonces la confidencialidad y la integridad son dos cosas diferentes. La confidencialidad indica mantener algo en secreto, mantener una información en secreto. Disculpen, tengo un inconveniente técnico con el micrófono, voy a cambiar de micrófono. Un momento, por favor.

Muy bien, ahora este micrófono funciona bien. Muy bien.

La protección de la integridad significa asegurarse de que una información sea la información correcta. Entonces acá les dejaba un ejemplo práctico para entender esto. Acá tenemos un recibo de transacción de cajero automático. Aquí tenemos en rojo el saldo de esta cuenta bancaria, esta es una información que no quiero compartir con todo el mundo, pero realmente no requiere confidencialidad.

No es el fin del mundo si la gente se entera del saldo de la cuenta bancaria, pero quiero asegurarme de poder verificar que esto sea cierto. Yo sé cuánto dinero tenía, luego hice una extracción de dinero y me queda este saldo. Entonces necesito verificar que

esto es correcto. Si el banco y yo hicimos los mismos cálculos, tendríamos que tener los mismos números.

Entonces esta es la protección de la integridad o la capacidad de verificar la información. La confidencialidad es como mi clave pin, mi número pin para ingresar al cajero. No importa cómo se me ocurrió el número, lo que me importa es que solo yo lo sé.

Bueno, otro ejemplo de integridad versus confidencialidad. En una elección, por ejemplo, a mí me interesa la integridad del resultado y no la confidencialidad. En realidad, no sería del todo útil tener confidencialidad porque todo el mundo quiere saber el resultado. Lo que queremos verificar es la integridad, es decir, que la persona que ganó, realmente fue la persona electa.

Ahora bien, lo que sí me interesa es la confidencialidad de mi propio voto, yo no quiero que los demás sepan a quién voté. Entonces tenemos que ver la seguridad de los objetos versus los canales también. La seguridad de los objetos es como, por ejemplo, tomar cierta información y cifrarla, encriptarla para que esté segura. Por ejemplo, yo puedo escribir una carta y la escribo en un código secreto y eso sería una seguridad de objeto para esa información.

Ahora bien, la seguridad del canal implica tomar esa carta y ponerla en un sobre y enviarla por correo en un sobre cerrado. Entonces mantengo la seguridad de la información en ese canal

en particular. Ahora bien, ¿cómo se relaciona esto con las DNSSEC y el DNS en TLS? Bueno, muy bien, las DNSSEC nos dan protección de la integridad. Aquí tenemos información pública, esta es una de las firmas para el sitio IETF.org. Esto es información pública, todos lo pueden ver, lo pueden verificar no tiene confidencialidad.

Ahora bien, al utilizar esta información pública podemos hacer algunas cosas que están muy buenas, por ejemplo, asegurarnos de que la información no se modificó en los servidores primarios o secundarios del DNS. Si me aseguro de que no se le modificó para nada en todo este gráfico desde la internet al ISP, también me aseguro de que el ISP no haya interferido con esa información. Me aseguro de que nadie la modificó y también en la última etapa que viaja desde mi casa al SIP y tampoco cambió esa información en mi red.

Hace poco vemos, por ejemplo, los enrutadores hogareños que se vieron afectados y entonces se hicieron cambios a la información, sin embargo, las DNSSEC no nos dan ningún tipo de confidencialidad. Esto significa que un atacante que está en internet entre mi resolutor e internet, puede ver exactamente la información que yo estoy mirando. No es del todo cierto, lo que pueden ver es que alguien está mirando determinada información.

Por otra parte, mi ISP puede decir quién está mirando una información. Entonces pueden ver que yo estoy mirando un nombre o que estoy buscando algo, un nombre en particular. Y esto se aplica al atacante que se interpone ente mi hogar y el ISP. Pueden ver lo que yo estoy buscando. Y también en mi red hogareña, en mi enrutador hogareño, el atacante puede ver qué es lo que yo estoy buscando.

Ahora bien, esto no parece ser un problema tan grave porque bueno, es tráfico en el DNS, ¿a quién le importa? Pero, en realidad, hay mucha información acerca de todo esto que es importante. Por ejemplo, si yo busco la página alcoholicosanonimos.org bueno, hay posibilidades de que yo necesite ir a una reunión de alcohólicos anónimos, entonces ya no soy tan anónimo. O si miro el sitio, o busco el sitio derechosgay.org, bueno eso revela algo de mi privacidad. Entonces quizás no sea tan deseable que esto suceda.

Y es más alarmante aun esto en algunos países donde uno busca información de algunos partidos políticos y sabemos que la historia no termina bien. Entonces en todo punto donde un atacante pueda ver lo que estamos buscando, también nos puede bloquear ese tráfico, entonces puede impedir que nosotros busquemos determinados nombres.

Entonces aquí vemos las cuestiones del DNS en el TLS, en HTTPS, etcétera. Ahora bien, todo esto nos brinda confidencialidad, entonces tenemos una manera de lograr que en mi enrutador hogareño y su conexión con mi proveedor de servicio de internet, yo logro la confidencialidad de mis búsquedas en internet. Nadie puede ver lo que yo estoy buscando. Desafortunadamente, en el resolutor esa información todavía es visible y mi ISP puede ver lo que yo estoy buscando. Y luego, desde el resolutor hacia el internet en público, bueno esa información es visible y los atacantes la pueden ver. Pueden ver lo que se está buscando.

El IETF está trabajando para mejorar esta situación de manera tal que se pueda hacer el encriptado de estas dos partes del circuito entre el resolutor y los servidores de nombre autoritativos o autorizados.

En algunos casos vemos que en algunos países hay censura. Esta es una fotografía bastante conocida, la primavera árabe. En Turquía se bloqueó el acceso a los resolutores locales. Con sus resolutores locales, Turquía bloqueó una serie de sitios web que los usuarios querían ver. Entonces esto lo pintaron en una pared justamente para que los usuarios cambien los datos en su DNS. Esto funcionó durante un tiempo pero también fue bloqueado posteriormente.

Aquí vemos cómo funciona esta tecnología, podemos encriptar ya desde nuestra casa, desde nuestros hogares, luego pasamos a nuestro ISP y estamos en un resolutor público fuera del país. Esto depende de ustedes, ustedes deciden si utilizan el resolutor de su ISP o el resolutor que ustedes deseen.

Desafortunadamente, su consulta todavía sigue siendo visible y, por último, en el último tramo, nuevamente estará encriptada.

Entonces de esto se trata tener el DNS en TLSs, que se gana cierta confidencialidad, pero no se puede proteger la modificación de los registros en los servidores del DNS antes de que se los envíen. Entonces si sus servidores de nombres secundarios no los manejan ustedes, tienen que confiar en que nadie los haya modificado. Tampoco se logra la protección para evitar que alguien modifique los registros en el resolutor en sí.

Entonces no importa el resolutor que utilicen, si ustedes no utilizan DNSSEC, entonces todavía se puede ver la información. Entonces es válido preguntarse por qué no podemos tener ambas tecnologías. Bueno, aquí vemos el resultado que tendríamos si utilizamos las DNSSEC y también el DNS en algunos de estos protocolos. Logramos la confidencialidad en todo el recorrido de la información y también un sólido grado de protección de la integridad de la información, con lo cual podemos verificar que logramos la respuesta que realmente estábamos buscando y,

básicamente, las DNSSEC les dan cierta protección y el DNS en protocolo TLS les dan otra protección.

Entonces para lograr la protección total, deberíamos utilizar ambas tecnologías. Bueno, esto puede parecer como mucho trabajo por hacer, pero la realidad es que si quiero tener un nivel de seguridad óptima, debo implementar ambas tecnologías. Y ahora si tienen alguna pregunta, las voy a recibir con todo gusto.

RUSS MUNDY: Gracias por la presentación. Tengo una pregunta, pero antes de eso quiero pedirles a todos los participantes que para los intérpretes y para la transcripción posterior, digan su nombre antes de hacer la pregunta.

Bueno, muy bien. Gracias, Warren. Cuando uno combina estas tecnologías, ¿qué ve o cuáles serían las posibles desventajas? Además de que es difícil y cuesta trabajo. ¿Qué otras desventajas podría haber al implementar ambas tecnologías?

WARREN KUMARI: Bueno, principalmente que hay que trabajar mucho más. Cada vez que uno agrega una capa de seguridad, también agrega un riesgo de falla. Entonces al trabajar con ambas tecnologías, estamos agregando dos posibilidades de fallas. Hay más probabilidad de que algunas cosas salgan mal. Pero realmente

vale la pena correr estos riesgos. Si tenemos estas dos tecnologías, existen por un motivo. No sé si con eso respondí su pregunta.

JACQUES LATOUR: Tengo una pregunta acerca de DNS-sobre-HTTP. ¿Eso agrega un mecanismo para verificar la integridad de las DNSSEC?

WARREN KUMARI: No, no. Tenemos dos tipos de servidores y, básicamente… pensemos como en una VPN una red privada virtual que estamos utilizando. Entonces una vez que el DNS pasa por TLS, no se lo puede modificar, no se puede modificar la información en curso. Sí se puede modificar en el punto de inicio en el resolutor.

No sé si respondí la pregunta. Veo su expresión y no estoy seguro de haber respondido correctamente.

JACQUES LATOUR: Entonces en Firefox, por ejemplo, ¿no se validan DNSSEC?

WARREN KUMARI: Bueno, tengo entendido que no.

JACQUES LATOUR: Sí, tenemos que trabajar al respecto.

WARREN KUMARI: Sí y creo que es razonable realmente tener DNSSEC y DNS en TLS. Y Vittorio dará una muy buena presentación sobre DNS-sobre-HTTPS y hay que ver si uno confía también en su proveedor de servicios de internet, eso es importante también.

JACQUES LATOUR: Muchas gracias, Warren. Y hay otra pregunta en la sala, a ver.

JOHN: Me llevó un tiempo darme cuenta de que una de las principales ventajas de las DNSSEC es que uno ya no se preocupa por el origen de los datos. Básicamente permite tener cierta tecnología en el DNS, pero si la firma de las DNSSEC es válida, uno no se preocupa por la raíz desde donde proviene esa información.

WARREN KUMARI: Bueno, claro. Una de las cosas que nos brindan los DNSSEC, es poder trabajar con DANE y mecanismos similares. Para esos mecanismos realmente hay que asegurarse de que obtuvimos la respuesta que realmente estábamos buscando. No queremos confiar en el resolutor para que tome estas decisiones en materia de seguridad para nosotros y eso permite generar otras cosas con

la información entre su propio titular y usted también y no queremos que nadie se interponga en ese camino.

JOHN: Entonces esto permite algunos caminos no confiables y complicados. Es como el protocolo TCP, uno en realidad no se preocupa de lo que pasa en el medio si realmente le llega la información correcta.

ORADOR NO IDENTIFICADO: El DNS-sobre-HTTPS hace que uno pueda validad el certificado y uno piensa que está hablando con el servidor de DNS que cree que es el correcto, pero lo que importa es la seguridad del objeto, ¿verdad?

JACQUES LATOUR: Okay, muy bien. Gracias a todos. Tenemos una pregunta de Geoff Houston, hay en participación remota. ¿Hay una diferencia entre TLS como transporte en una transacción del DNS o en utilizarla como objeto de HTTP?

WARREN KUMARI: Hay una diferencia, pero creo que me llevaría demasiado tiempo responder aquí y ahora. A menos que alguien quiera responder a esa pregunta.

JACQUES LATOUR: Vamos a escuchar la presentación de Vittorio antes y le agradecemos a Warren por su presentación.

Nuestro próximo orador es Vittorio Bertola de Open-Xchange.

VITTORIO BERTOLA: Mientras proyectan mi presentación en pantalla… Diría que más que una presentación, es una serie de reflexiones que me surgieron en la semana pasada en este debate sobre DNSSEC versus DNS en HTTPS.

No sabía que se iba a presentar. Reconozco que el orador anterior hizo un buen resumen. Todos llegamos a la conclusión entonces de que necesitamos estas dos cosas porque son dos cosas distintas. Cuando hablamos con gente que no conoce tanto DNSSEC, a lo mejor piensa que no necesitan los dos y quizás en esto haya cierto mérito. ¿Cuál es exactamente la diferencia entre ambos?

Entonces rápidamente voy a hacer los siguientes puntos saltando lo que ya dijo Warren. La diferencia entre DNSSEC y DNS-sobre-HTTPS. Son distintos en su concepción y en el momento en que se concibieron. Aparentemente, uno de los requisitos claves era encontrar una manera de asegurar la integridad sin tener que encriptar todas las comunicaciones porque se consideraba al

principio que era un problema en especial en lo que hace a la carga computacional.

Entonces podemos preguntarnos por qué nos encriptaron las comunicaciones como se hace hoy día. Bueno, porque es un modelo que existe desde hace menos años. En aquella época no era la tendencia. Eso es lo que me han comentado algunas personas.

Veamos qué hace todo esto. Nos dice que podemos confiar en la respuesta. El objetivo es que el cliente reciba datos confiables, que uno pueda confiar en que lo que recibe no ha sido alterado por partes en el tránsito en el camino. Da seguridad al objeto.

DNS-sobre-HTTPS es distinto porque encripta las comunicaciones, encapsula el DNS en la comunicación, toda la comunicación está encriptada. Esto brinda confidencialidad, es distinto de DNSSEC. Obviamente el costo computacional es mayor pero eso ya no es un problema hoy día. Y brinda seguridad del canal, es decir, el canal que se usa para comunicarse con el resolutor.

La gente entonces dice, ‘este canal es seguro, nadie puede alterar mi respuesta y también me garantiza que la respuesta no ha sido alterada’. En definitiva es lo mismo, entonces la gente ha empezado a decir, ‘bueno, son dos mecanismos de seguridad

distintos, pero en definitiva el resultado final es que nadie manipule, altere mis respuestas'.

Entonces ¿por qué no podemos usar esto en lugar de DNSSEC? Y es una propuesta muy atractiva porque si decimos que el nivel de garantía de la seguridad es el mismo, tenemos más confidencialidad y más integridad con DNSSEC que las tecnologías anteriores no brindaban y además es más fácil de implementar. Entonces la gente dice que no obstante, DNSSEC es difícil de administrar.

Pero eso no es tan así. Aquí hay en esta idea hay una falacia. Lo que quiero resaltar es que la diferencia reside en qué se puede confiar, ¿en qué fuente de información se puede confiar? DNSSEC brinda seguridad en el sentido de que la respuesta no ha sido alterada en toda la cadena, comenzando por la zona del servidor de nombres autoritativos a través de toda la cadena.

En DNS-sobre-HTTPS solo tenemos seguridad del resolutor. La respuesta si no fue alterada, pero desde el resolutor. Por lo tanto, la conclusión a la que podemos arribar es que si queremos tener tanto seguridad del canal como de los datos y tener tanto integridad como confidencialidad, hay que tener ambos.

Pero es tan así porque es una cuestión de saber en quién confiar. La cuestión en estos dos modelos es que la confianza en la fuente de la verdad, es el sistema de servidores de raíz en DNSSEC,

asegurarse de que todo esté adecuadamente validado. Es el sistema de servidores raíz el que nos dice la verdad.

Mientras que en DNS en HTTPS el oráculo o la fuente de la verdad, está en manos del resolutor. O sea, la verdad es aquello que nos dice el resolutor y en DNS, entonces en HTTPS no se hace validación por DNSSEC.

El problema es, ¿cuál es la verdad hoy día en el DNS? ¿Dónde está? El DNS se concibió como una base de datos distribuida, entonces sería decir que una respuesta correcta de un query del DNS sería una sola la correcta y todas las demás falsas. Mucha gente habla de las mentiras del DNS terminología similar lo cual es comprensible, yo no lo objeto, pero la realidad es que incluso hoy día las respuestas de las queries dependen mucho de quién es uno y a dónde estamos enviando la consulta, qué resolutor estamos usando.

O sea, en definitiva, la comunidad del DNS dice que esto no es más que un atajo y lo hacemos por muchísimas razones diferentes. Son distintos los motivos por los cuales los resolutores nos mandan distintas respuestas. La censura es solo una minoría de los casos de uso para modificar las respuestas en todos los niveles. La gran mayoría de los cambios tiene que ver con cuestiones de seguridad; nombres locales y cosas así.

El administrador a nivel del resolutor incluye la seguridad para trazar un perímetro para asegurarse de que los datos no salgan de ese perímetro para propósitos de este tipo. Hay otros casos que están relacionados de manera voluntaria, no ir a lugares que estén fuera de la red, por ejemplo, en la compañía que impide que los empleados se conecten a Facebook en horario laborable o una familia que no quiere que sus hijos entren a sitios web inapropiados. Hay incluso casos en que los gobiernos bloquean sitios, pero no lo hace por censura, por otros motivos, por ejemplo, porque hay evasión de impuestos y demás.

Y también las CNS's las redes de entrega de contenidos, también dan respuestas diferentes dependiendo de dónde uno se encuentre y quién uno sea. Una de las tendencias que vemos o preguntas, es si podemos seguir considerando el DNS como una base de datos distribuida. De esta base de datos vamos a leer, el DNS es algo mucho más complejo, es un servicio donde el mecanismo anticipa algún tipo de localización o distintos niveles de complejidad en las respuestas.

Si empezamos a plantearnos estas preguntas, la pregunta de cuál es la verdad, es muy relevante. Y cuál es la verdad en DNS y también cuál es la fuente de la verdad, es una pregunta relevante. Ahí podemos empezar a hablar si realmente necesitamos esta integridad a través de toda la cadena y del sistema de servidores raíz.

La cuestión es que hoy día se espera confianza en el resolutor. Muy pocos sistemas hacen verificación del DNSSEC en el dispositivo. La mayoría confían en que el resolutor haga esta verificación. Y si este es el modelo, bueno hay que confiar en el resolutor, esperar que no nos mienta. Porque uno no está chequeando que lo que uno recibe, es válido según el DNSSEC.

Y lo que mostró Warren, las imágenes de la integridad y la confidencialidad está muy bien, pero el requisito de que la validación se haga en el dispositivo es una exigencia. En este modelo que usa DNS-sobre-HTTPS quizás se conecte a un resolutor distinto, entonces cada aplicación individual tendrá que implementar validación. No es cuestión de implementar en el sistema operativo, será cada aplicación que hace una query y que tendrá que tener validación, sería fantástico, pero me pregunto si es algo realista y si lo es, cómo podemos hacerlo.

A lo mejor esto tampoco es la forma porque si aceptamos el modelo de confiar en el resolutor, tenemos esta DoH y la convención de confiar en el resolutor, entonces el resolutor tendrá DNSSEC y verificará todo lo que reciba de los resolutores autoritativos y eso podría estar bien, pero también está el caso de disrupción que es una preocupación del GDPS.

(Pido disculpas porque creo que los traductores están enloqueciendo.)

Bueno, este caso de disrupción de DNS-sobre-HTTPS es una manera de que el operador del resolutor sea el dueño del espacio de nombres, entonces si vamos a un modelo donde el resolutor es la fuente de la verdad, el resolutor así puede decidir qué nos puede contar. Incluso ni siquiera usar el sistema de servidores de nombres, usar o configurar TLDs nuevos.

Me han dicho que esto es una posibilidad aunque todavía no ha ocurrido. Yo lo aceptaría pero esta es una de las preocupaciones que surgen de este nuevo modelo de despliegue de DNS-sobre-HTTPS pero es otro caso que puede darse.

Como decía entonces, esta presentación no era más que una serie de preguntas y reflexiones que pretenden disparar la discusión. Si nos ponemos en el lugar del usuario, sí, todos confiamos en el sistema de resolutores de la misma manera que podemos confiar en el fabricante del browser favorito. ¿Los usuarios realmente quieren que la ICANN dé su bendición a las queries validadas o a alguna otra entidad?

Y otra pregunta es, uno de los temas taller era cómo hacer que los navegadores implementen DNSSEC. ¿Existe alguna razón por la cual los navegadores deban hacer esto? Quizás simplemente hacer DoH y asegurarse de que el resolutor implemente DNSSEC. Yo creo que es necesario discutir si el modelo de DNSSEC regional es válido, por ejemplo, los requisitos de que DNSSEC que eran

relevantes hace 15 años ya no lo son tan así. Hay nuevos requerimientos como el de confidencialidad un requisito que no era tan importante hace 15 años.

Esto a mí me hace pensar que quizás debamos empezar. En lugar de poner más protocolos y más cosas en esta pila del DNS, no sé si debiéramos repensar los requisitos y diseñar algo que cumpla todo, de lo contrario seguiremos emparchando y, a lo mejor, lleguemos a tener algo que sea totalmente inmanejable. Gracias.

JACQUES LATOUR: Gracias. ¿Alguna pregunta?

AFIFA ABBAS: Soy Afifa de Bangladesh. Hola a todos. Pregunto, para lograr tanto la confidencialidad como la integridad usted y Warren mencionaron que necesitamos ambos. Mi pregunta es, a ver, no hay ninguna razón o la segunda opción DNS en HTTPS permite que no haya forma de alterar el tráfico. ¿Es razonable usar ambos? Y si lo hacemos, ¿hay alguna posibilidad de agregarle latencia adicional a la red?

VITTORIO BERTOLA: La respuesta oficial es que sí, hay que hacer ambos porque se supone que cumplen distintos propósitos. Yo lo que quise decir

es que a lo mejor tendríamos que pensar en distintos temas, pero en definitiva tenemos que tener ambos. El DoH o el DNS-sobre-HTTPS hay muchas cuestiones de política que resolver, así que primero hay que tener conocimiento de los problemas antes de empezar a hacer la solución. Pero DoH brinda algo que DNSSEC no brinda.

Con respecto a la latencia, depende. Uno de los temas de DNS-sobre-HTTPS es que promueve cierta descentralización. Muchos de los resolutores en los ISPs locales van a usar otros resolutores remotos como el de Google y esto va a generar más latencia, dependerá de la conectividad porque las consultas al DNS van a tener que viajar más lejos, pero esto no necesariamente significa que sean más lentos, esto dependerá de la conectividad.

BARRY LEIBA: Ha sido difícil seguir su presentación porque usted hablaba muy rápido. En definitiva entiendo que usted está proponiendo un mecanismo híbrido donde el resolutor recursivo verifica DNSSEC desde el servidor autoritativo y nosotros usamos HTTPS para manejar la comunicación con el resolutor recursivo. Y confiamos en el recursivo para no tener que verificar DNSSEC en esa etapa. ¿Está proponiendo esto, usted?

VITTORIO BETROLA: Pido disculpas. Es algo que todavía está por ahí. La idea no es algo que me resulta totalmente claro, no es algo que yo esté proponiendo, estoy analizando las distintas posibilidades y me interesa saber qué piensan ustedes porque creo que es interesante, pero también creo que es un modelo que puede funcionar, genera esta cuestión de confiar en el resolutor.

Hay que elaborar también políticas para saber cómo elegir el resolutor, trabajar bajo la presunción de que hay que trabajar con un único resolutor. Hay gente que le gusta distribuir las consultas en muchos resolutores, así que es demasiado prematuro hacer ninguna sugerencia ahora, pero es algo que podríamos considerar. En especial ya que ahora estamos hablando de cuestiones de políticas entre la GNSO sobre HTTP, o sea, a lo mejor podemos considerar distintas hipótesis y no esperar a que pasen 10 o 15 años más.

¿Warren?

WARREN KUMARI: Imagino que seguiremos hablando de esto en el IETF y en otros foros, pero Vittorio planteó algunas inquietudes y me gustaría hablar del tema de los navegadores. El tema de que ellos deban usar esto.

Google en su momento dirá algo. Me pregunto si hay una serie de planes o deseos que adherir y una cosa importante es no sorprender a los usuarios. Entonces mi consideración es si un usuario ya tiene un resolutor configurado, ¿consideran testear si ese resolutor que usa el usuario está haciendo un uso oportunista? Y también que no haya planes de traspasar el resolutor sin el consentimiento del usuario. Creo que es una preocupación muy importante porque hay mucho interés.

JACQUES LATOUR: ¿Wes? ¿O quién quiere hablar primero?

WES HARDAKER: Mi micrófono está abierto así que gano yo. Interesante la presentación, interesante cadena de reflexiones. Me llama la atención el hecho de que los usuarios tengan que confiar en los navegadores. La realidad es que los usuarios tienen una confianza transitoria en quien les brinda la resolución porque en este momento los proveedores de navegación no son los que hacen resolución. A lo mejor tienen acuerdos. La mayoría como, por ejemplo, Firefox tienen a asociaciones.

Hemos tenido casos notorios de usuarios que no han podido tomar decisiones informadas de confianza y esto nos pone en un predicamento interesante porque los usuarios confían en sus

navegadores mucho más de lo que dicen porque esa asociación puede falsificar solicitudes. Estamos confiando más en el navegador de lo que usted potencialmente sugiere que se haga.

VITTORIO BETROLA: Antes de pasar a la otra pregunta, quiero aclarar que esto no era para forzar a los navegadores. Entiendo cuál es el abordaje de Google, pero es cierto, en definitiva toda esta arquitectura tanto en términos de gobernanza y tecnológicos, los servidores de nombres raíz es muy complicada. Si los usuarios tiene que elegir en quién confiar, bueno, es muy probable que ahí aparezcan en primer lugar los navegadores.

JACQUES LATOUR: ¿Si tenemos más preguntas…?

STEVEN CARR: Entiendo de dónde viene toda esta tecnología pero tenemos que estar seguros de que lo siguiente no ocurra, que los navegadores asuman el control. El DNS es el protocolo subyacente. Hacer todo esto en el navegador para mí es el lugar que no corresponde, es incorrecto. Hay muchísimas otras aplicaciones en el sistema operativo que dejarán de estar protegidas con esta tecnología.

Entonces, como decía Warren, en tanto y en cuanto los navegadores tengan un mecanismo que les permita determinar si el sistema operativo ya es seguro y que lo potencien, bien, pero que el navegador suplante o asuma el control de la seguridad, no debiéramos caer en esta trampa porque ahí los usuarios tendrán un sentido de identidad falso. Podrían tener seguridad del navegador, pero todo lo demás que ocurre en el sistema, no lo es.

JACQUES LATOUR: Por eso estamos hablando de este tema ahora. No sé si usted quiera agregar algo, Warren.

WARREN KUMARI: Aparentemente cada vez más las aplicaciones harán su propia resolución del DNS, tanto si la gente cree que esto es una buena idea o no. Aparentemente el curso es por ahí. Y yo creo que esto se debe a que hay cambios de las aplicaciones y la gente va decidiendo que esto es lo bueno, no sé si es lo correcto.

Como ejemplo, desde hace tiempo ya, la aplicación de Netflix y otras, vienen haciendo su propia resolución. Es muy fácil hacer resolución propia y es un cambio definitivo de la arquitectura que es algo que debiéramos investigar y discutir.

Pero no es una cuestión de navegadores versus sistemas operativos, creo que es aplicaciones versus sistemas operativos.

Es mucho más amplio, pero es un tema a discutir. Y para la gente que vaya a la IETF, habrá una reunión específica sobre este tema y en este debate hay muchísimos subtemas.

VITTORIO BETROLA: Comparto sus preocupaciones y yo estoy en el IETF, una de las personas que promueve este debate.

Otro comentario que quería hacer es que no todas las aplicaciones podrán hacer resolución propia. Si sacamos todo la seguridad que se hacer a nivel del resolutor y lo pasamos al extremo de la aplicación, el problema es que no sé, con la internet de las cosas una heladera no podrá hacer resolución. O sea, hay problemas graves en términos de seguridad que no se pueden manejar solo con la solución a través de las aplicaciones.

JACQUES LATOUR: No hay más preguntas, entonces le damos las gracias a Vittorio por su presentación.

Ahora vamos a escuchar a Duane Wessels de Verisign que hablará del análisis posterior al traspaso de la KSK.

DUANE WESSELS: Muchas gracias, Jacques. Quiero compartir algunos datos con ustedes que recopilamos después del traspaso de la KSK. Aquí

vemos las fechas clave hasta el día de hoy, todavía queda una fecha clave por delante, pero quiero focalizarme en lo que sucedió el 11 de octubre que fue, efectivamente, cuando se traspasó la KSK. Y el 11 de enero que fue cuando se publicó la clave.

Muy bien, estos datos provienen de distintas fuentes. En primer lugar, vemos tráfico de consultas al DNS hacia los servidores raíz operados por Verisign, también vemos señalización de etiquetas clave para esos mismos resolutores conforme al documento técnico RFC correspondiente.

Entonces aquí tenemos gráficos de consultas para el protocolo DNS KEY en la raíz. Entonces este gráfico nos muestra qué sucedió un poquito antes del traspaso e inmediatamente después del traspaso. Aquí tenemos millones de consultas o queries por día, entonces antes del traspaso veíamos de 10 a 15 millones de consultas diarias y después del traspaso teníamos o vimos de 70 a 80 millones por día. Y vemos que a lo largo de los días posteriores de los cambios en los tiempos de vida, vemos que hay un pequeño incremento.

En este gráfico vemos las direcciones IP individuales. Incluí esta información para mostrar que estas direcciones IP tienen distinto tipo de comportamiento; algunos tuvieron un pico de actividad muy breve, luego esa actividad disminuyó. Entonces no fue

realmente mucha ayuda ver a las direcciones IP individuales porque tenían comportamientos diferentes.

Aquí vemos los cambios cuando sucedió la revocación. Vemos que al momento de la revocación, vemos un incremento significativo. Esto sucedió durante los 10 a 12 días posteriores a la revocación. Luego vemos lo que sucedió un mes después, vemos que sigue incrementando. Siguen incrementando los datos y vemos ahora que estos servidores raíz reciben mil millones de consultas por día en DNS KEY. Es decir, que esto aumentó 100 veces en comparación a antes del traspaso, entonces vemos que hay un aumento significativo.

Obviamente esto va a seguir incrementando y, a medida que esto suceda, estaremos frente a un problema cada vez mayor. Entonces si ustedes pueden comunicarse con las redes donde se originan estas consultas, sería interesante llegar a las causas raíz para solucionar estos problemas y detener este tipo de tráfico de consultas.

Aquí vemos otra vez un gráfico donde se ve el distinto comportamiento de las direcciones IP individuales.

Y hay una pregunta que surge al respecto. ¿Este cambio se debe a que hay muchas respuestas en protocolo IPv6? Y la magnitud es de 1425 bytes en este momento, mucho más grande que

anteriormente y es mucho más grande que el tamaño mínimo en protocolo IPv6 que es de 1280 bytes.

Pero, aparentemente, esta no sería la razón. Es decir, vemos de 10 a 100 consultas por segundo en algunas fuentes, pero lo vemos en el protocolo IPv4 y en el protocolo IPv6. Entonces esto en realidad parecería ser una situación que se da inmediatamente después del traspaso y que luego va a desaparecer, en inglés es rollover and die.

Ustedes recordarán esta situación y esta definición. Hace 10 años el registro regional RIPE estaba haciendo mantenimiento o estaba a cargo de mantenimiento en zonas en .arpa entonces utilizaban anclajes de confianza que se configuraban manualmente y cuando los usuarios y operadores retiraban manualmente las claves de cada una de sus zonas, surgían estos picos de actividad que a mi juicio son muy similares a la situación que estamos viendo ahora.

Ahora vamos a ver algunos gráficos que nos van a ayudar a visualizar estos datos y también tengo algunas imágenes preparadas. Pero antes quiero entender justamente un poco más cuáles son las fuentes de consultas y qué clase de consultas se están formulando, pero tenemos que ver si son solo consultas de DNS KEY o si son de otro tipo. Entonces la idea es tener gráficos

de dos ejes en el cual en un eje se muestran las consultas de DNS KEY y en el otro eje las consultas de otro tipo.

Si ustedes hacen esto, se ve de esta manera. Sería la forma más sencilla de hacer este gráfico, pero no se ve con claridad porque vemos que todos los datos están donde convergen los dos ejes. Con lo cual podríamos hacer el gráfico de esta otra manera, pero también vemos que aun así hay mucha superposición entre los datos.

La idea es tratar de distribuir mejor estos datos de manera tal que los puntos que representan datos en el gráfico estén todavía mejor distribuidos. De todas maneras sigue habiendo mucha densidad de información, entonces cambié el tamaño de los distintos puntos que representan a los datos en el gráfico y ahora podemos tener una visualización mucho más clara.

Ahora que saben o entienden cómo funcionan estos gráficos, notarán que hay una línea diagonal y les reitero, cada uno de estos puntos es una dirección IP. Cada hora, por ejemplo, y cada punto que está por debajo de esta línea realiza consultas sobre clave en contraposición a las otras consultas, realiza más consultas sobre claves, acerca de claves key queries.

Entonces ustedes van a ver que normalmente un servidor de nombre recursivo estaría aquí en esta parte del gráfico donde hay

una cantidad muy pequeña de este tipo de consultas y muchas otras consultas de otra clase que no son key queries.

Ahora quiero mostrarles otra parte de mi presentación, quiero mostrarles una visualización, una imagen. Disculpen, estoy buscando la imagen que quiero compartir con ustedes.

Bueno, aquí tenemos el gráfico con una animación que es para un traspaso de la clave para firma de zonas ZSK. Entonces en esta línea representamos el tiempo. En realidad no es un traspaso de ZSK, sino que en realidad se trata de la publicación previa de esta clave ZSK en la zona. La clave para firma de zona.

Van a ver que hay muchos puntitos que se mueven, parece que están como bailando ahí cerca de la línea diagonal y, aparentemente, antes y después del evento todo está igual, pero si miramos en mayor detalle, vamos a ver que hay algunos puntitos en verde que representan IPv6 y el color violeta representa IPv4. Van a ver que tenemos como estos grupos o estas bandas de puntitos en color verde que representan a IPv6. Entonces hacen una consulta para llevar a la clave, de repente esa consulta se ve interrumpida y luego lo vuelven a intentar.

Entonces parece que hay como dos consultas por fuente de dirección IP y eso sucede en múltiples ocasiones. Y bueno, también el gráfico animado les permite ver otros aspectos interesantes. Si miramos aquí donde estoy señalando, vemos

este punto que aparece y desaparece. Bueno, aparentemente, hay miles y miles de consultas desde esa fuente y luego desaparecen, con lo cual tenemos un pico de consultas muy, muy breve en algún momento.

Y luego, tenemos alrededor otros puntos también que aparecen y desaparecen y se superponen unos con otros, lo cual para mí es interesante. Aquí les señalo otro aspecto para tener en cuenta en otros gráficos. Creo que esto se originó en Corea, que la fuente es en Corea, pero no tengo demasiada información al respecto.

Bueno, este gráfico animado corresponde al momento del traspaso, al momento en que se dio el traspaso. Van a ver que hay un descenso de actividad y luego la actividad se retoma y vuelve a incrementarse. Entonces, supuestamente, o lo que debe haber pasado, es que después del traspaso tuvieron algún problema con la resolución, durante un par de horas tuvieron que resolver esos inconvenientes y luego retomaron su actividad normal.

Voy a volver al principio y les señalo esta parte de la animación con muchos cambios y muchas fuentes de consultas que se tornaron cada vez más y más activas y empezaron a enviar muchas, muchas consultas, muy diferente de este otro momento que les había mostrado.

ORADOR NO IDENTIFICADO: Duane, ¿puede explicar este comportamiento de las consultas entre todos estos clientes?

No, por ejemplo, las consultas de DNS KEY y las otras consultas.

DUANE WESSELS: Ah, se refiere a esta línea diagonal aquí. Bueno, realmente no se lo puedo explicar, pero si uno piensa en el comportamiento esperado después de un servidor de nombre recursivo, uno vería por día una consulta DNS KEY por TTL por ciclo de vida. Todo lo que está en esta otra parte del gráfico animado, no es normal. Probablemente se trate de alguna herramienta como un servidor de nombre en caché, en memoria caché. Pero esto que vemos aquí no refleja el comportamiento normal de un servidor de nombre recursivo. Quizás se trate de alguna prueba, de alguna medición. Aparentemente hay muchas fuentes de consulta que en realidad están haciendo mediciones y me cuesta creerlo.

JACQUES LATOUR: ¿Esto es para los IP que están haciendo? ¿Qué consultas?

DUANE WESSELS: Son para los IP originarios que están haciendo esta consulta que son la fuente de consulta. No todos los IP.

DANIEL MIGAULT: Con respecto a las consultas, por ejemplo, cuando pasó lo de .arpa y sucedió esa situación que usted nos explicó en ese momento con .arpa. ¿Entendemos la situación y por qué sucedió?

DUANE WESSELS: En un minuto se lo respondo. Este gráfico animado muestra el período alrededor de la revocación de la clave, entonces al final del traspaso, tenemos mucha actividad. La revocación fue un cambio muy, muy abrupto, entonces muchas de estas fuentes de consultas realmente registraron muchísima actividad y empezaron a formular muchísimas consulta de DNS KEY.

Con respecto a esta parte del gráfico animado, realmente no entiendo qué es lo que está sucediendo y no lo puedo explicar.

JACQUES LATOUR: Puede ser un virus o un gusano.

DUANE WESSELS: Sí, podría ser, pero bueno hay que ver de qué se trata. Estos datos siguen aumentando y los tengo registrados hasta el 15 de enero. No tengo datos actuales pero en las últimas semanas vimos un incremento significativo en este tipo de datos. Lo que les estoy mostrando ahora es justo después de la revocación.

ORADOR NO IDENTIFICADO: ¿Cuántos IP van pasando de una parte del gráfico a otro? ¿Más de 100.000?

DUANE WESSELS: Yo diría que sí, que más de 100.000.

Bueno, debería continuar con mi presentación. No sé cuánto tiempo me queda.

Muy bien. Entonces yo incluí unas imágenes del antes y el después del traspaso de esta clave para la firma de zona ZSK. Lo pueden tener como futura referencia. Y voy a tratar de responder la pregunta de Daniel.

Usted se preguntaba acerca de lo que sucedió con el .arpa. Bueno, en aquel momento se publicó un informe acerca de lo que sucedió y, básicamente, se hacía validación de DNSSEC y la validación falló porque ya no estaban las claves disponibles, entonces se seguía intentando agresivamente una y otra vez, una y otra vez.

Y fue antes de IPv6 y creo que incluso fue peor de lo que le estoy contando porque la idea era hacer lo siguiente. Supongamos que había una búsqueda en .com y había dos servidores de nombre. Se multiplicaban todas estas consultas de manera exponencial y se seguía intentando, intentando, intentando con las consultas

de manera muy agresiva y se las guardaba en memoria caché negativa solamente por tres segundos.

Entonces cada una de estas consultas terminó enviando decenas y cientos de consultas a la raíz. Entonces creo que hubo un comportamiento similar con otras tecnologías. Bueno, en fin, no le puedo dar más detalles, pero creo que sigue habiendo otros problemas allí.

WARREN KUMARI: Y creo que en ese caso ellos estaban haciendo lo que ellos creían que les indicaba el documento técnico RFC para este caso, creo que ese fue el problema también.

DUANE WESSELS: Bueno, nosotros hicimos lo siguiente: tomamos la lista de direcciones IP que formulaban estas consultas y les pedimos su versión en .bind. A veces yo no confío tanto en estos datos, pero de todas maneras sirven a título informativo.

Hay muchas versiones antiguas de BIND. Tampoco obtuvimos muchas respuestas pero bueno, hubo quienes estuvieran más abiertos y más dispuestos a responder y esta es mi información que logramos obtener.

Ahora voy a hablar acerca de los datos sobre señalización de etiquetas clave. Esto sucedió justo en el momento de la revocación. En color verde vemos fuentes que indican tener la clave antigua y la calve nueva en azul. Indican tener solamente la clave nueva, entonces uno diría, 'Hm, estas cifras tan pequeñas indican que esto se configuró manualmente y que cambiaron de claves manualmente'.

Aquí en esta línea marcamos el momento de la revocación y vemos que en una hora, aproximadamente, la mitad de estos señalizadores de etiquetas clave cambiaron los datos que estaban enviando. Y en color rojo vemos a quienes tenían solamente la clave antigua y no cambió su nivel de actividad, después dela revocación solamente le prestan atención al documento RFC 5011.

Entonces hay uno interesante también y ver, por ejemplo, la revocación de la clave de 2010 y la clave de 2017. De hecho, este documento RFC no era demasiado claro, no tenía instrucciones demasiado claras acerca de cómo gestionar el tema de una clave revocada en el conjunto de anclajes de confianzas. Y luego están también los que dijeron que tenían una sola clave revocada en su conjunto de anclajes de confianzas.

Y aquí tenemos también datos que nos muestran que todavía tenemos actividad en el orden del 10% en cada una de estas categorías.

Bueno, esta diapositiva reitera lo que ya les conté y las últimas diapositivas son un tanto confusas, pero lo que quise hacer fue combinar estos datos y ver qué sucede con los señalizadores que están en este nivel de DNS KEY en los top talkers y vemos distintas combinaciones de etiquetas clave y vemos, por ejemplo, que en algunos momentos tuve este tipo de datos o este otro. Y vemos entonces que sucede de las fuentes de las cuales provienen la mayor cantidad de consultas.

Vemos que en algunos casos hay más estabilidad, vemos que también en otros casos son un poco más dinámicos. Nosotros no vemos los informes a diario, sino que los recibimos cada tanto. Quizás se trate de actividad en dispositivos móviles.

Bueno y con esto finalizo mi presentación. Ya respondí algunas preguntas y, si tenemos tiempo, voy a responder más.

JACQUES LATOUR: Vamos a tomar las preguntas después de Wes.

Gracias, Duane.

WES HARDAKER: Soy Wes Hardaker de la USC el ISI y voy a hablar de algunos datos que nosotros vimos en nuestro servidor raíz.

Yo tengo una adicción que es la creación de gráficos, que no entiendo, así que lo que van a ver hoy, voy a compartir mi adicción. Ya he presentado materiales y me han brindado respuestas, entonces ahora voy a hacer lo mismo, voy a presentar gráficos que no entiendo pero voy a usar poco tiempo porque tengo hambre.

Entonces comenzaré con un análisis de una semana de datos, voy a hablar de algunos clientes individuales que pensamos son interesantes, son datos que también podemos poner a disponibilidad porque nos interesa saber la comparación. Esta semana de datos va desde el 9 al 16 de enero de este año. El conjunto que se revocó el 11 de enero… Así se ve la semana de datos, como ven es muy periódico el gráfico. Hay varios puntos que hacen unos picos extraños arriba, me referiré a ellos al final de mi presentación. Primero voy hablar de la semana de datos, pero como la mayoría del gráfico, suben y bajan, suben y bajan.

Aquí vemos solo las consultas de la DNS KEY. La mayoría de estos gráficos mostrarán esta línea vertical que es el 11 de enero. La verdad no estoy seguro por qué esta está caída. Gran parte de esta presentación la preparé la semana pasada y tenía muchas otras tareas que hacer y ya me hicieron preguntas por qué está

esta caída, no me pude ocupar. Mi idea es que estos datos son datos que están rotos. ¿Por qué hubo gente que hizo menos consultas después de la revocación? No sé por qué.

Este es el número de consultas de la DNS KEY por hora. Ven que como una rampa. Los datos a la derecha están un poquito más arriba que los de la izquierda. Otra cosa que estaba buscando es lo siguiente. Bueno, cuando se hace una consulta de la DNS aquí, ¿qué se está pidiendo? La mayoría estaba recurriendo a la raíz, pero también había consultas de otros nombres populares como net y arpa.

Por lo general, si analizamos el comportamiento de los resolutores, es inusual que se pidan KEYS distintos de esto. Imagino que aquí la razón por la que se pidió el dlv.isc.org es porque ya hace dos años que está caído y se estaba buscando la validación. No se tendría que estar pidiendo la clave en principio porque tendría que estar pre configurado, la verdad no sé qué está pasando acá.

Entonces cuando empecé a desglosar—volvamos a este gráfico—cuando dividí estas consultas y las asigné a direcciones individuales para ver de dónde venían la mayor cantidad de consultas, vemos que hay un pico el 11 de enero. Cada uno de estos colores representa una dirección distinta. Algunas

direcciones tienen una rampa que sube bastante rápido y hay pedidos de DNS KEY en mayor número.

Pasemos ahora a los colores más interesantes. Este es el que más se comunicó, el número 1 que estaba preguntando: "¿Hay alguien ahí? ¿Ya llegamos ahí?" Hay alguien que pidió la clave repetidamente hasta que nadie le contestó y se aburrió y se fue y este es el problema. El problema desde el principio. A la izquierda—perdón, a la derecha—se ve el comportamiento normal. Se ve que alguien andaba sondeando, indagando, o tratando de monitorear el evento.

El número 16 en términos de los que más consultas hacían, tuvimos este incremento gradual. Bastante bajo al principio, incluso a nivel 0 y luego estos pedidos duraban 5 minutos. Luego hay una rampa ascendente y después permanece en un nivel bastante constante.

Esto es interesante que probablemente esté relacionado con esta conducta de sondeo.

Esta actitud de problemas tempranos, o sea, asumir que hay un problema y luego aparece ahí en el gráfico y vemos que el problema era porque estaba hablando o comunicándose antes del evento. Hay gente que después tuvo problemas al final del período. No sé por qué porque los resolutores tienen que resolver en los primeros dos días, hacer una caché según el

tiempo de vida y ahí es donde se espera que el problema ocurra, pero no fue así el caso. Y, de hecho, sobre esto vamos a hablar después.

En este caso hay muchos puntos arriba y muchos puntos altos y muchos puntos bajos en el mismo período temporal. Que es interesante porque indica que preguntan mucho en los primeros 5 minutos y después no preguntan nada o casi nada en el mismo periodo de 5 minutos. No sé por qué.

El número 76 preguntaba mucho al principio, hizo un silencio dos o tres días, justo en el período de revocación y después empezó a preguntar mucho otra vez. No, como dije antes, estos gráficos no les puedo dar una explicación de por qué es así, solo puedo compartirlos y mostrarlos. Hubo varios casos donde la gente iba empeorando con el tiempo y había patrones como escalonados, este es un ejemplo de ello.

Hay una gran población de zonas en el mundo que sabe que si muchos resolutores envían a una única dirección, aparecen cosas como esta. Estos escalones se van desapareciendo después de dos días. ¿Por qué es así? No estoy seguro. A veces las cosas mejoran. Puede ser porque hay cosas que se interrumpen o porque la gente sabe dónde está el problema, entonces empieza a descender la curva.

Este es el que más consultas tuvo el número 1. Consultas de hasta 15.000 cada 15 minutos. Un patrón muy interesante de picos, diría que 1 por día. Y lo único que pedía aquí era la clave de DNS KEY y yo me preguntaba qué más está preguntando y no, nada más, solo pedía la clave. Así que todo esto después está en la parte de texto.

Este es mi favorito. No porque es el 007, sino porque duró mucho y después cayó a niveles que no son del todo irrazonables y después volvió a subir.

Estoy tratando de entender esto. Tuvimos muy poca visibilidad. En lugar de analizar los pedidos originales, la mayoría de estos casos solo pedían la clave del DNS KEY y hay muy poca visibilidad de qué otra cosa está pasando. Entonces podemos decir… Muy bien, hace dos días yo dije: "¿Qué pasaría si miráramos los índices de consulta? La velocidad mínima y la velocidad máxima". Porque como dije antes, hay consultas que se hacen muy rápidamente y otras que no se hacen rápidamente. Estas entonces son las velocidades máximas y mínimas por hora.

Como ven está ese punto verde que es gigante a la derecha y hay una velocidad mínima, es decir, para cada punto hay un punto violeta y verde correspondiente. No están las referencias, les pido disculpas. No puse la línea vertical. Bueno, hay muchas

cosas que se pueden mejorar aquí. Lo que quiero mostrar es que hay una brecha significativa entre el mínimo y el máximo, eso indica que muchas máquinas hacen muchas consultas y hay otras que no hacen consultas frecuentes.

Si sacamos los valores excedentes o que están fuera del patrón, hay un gran número de máquinas y de paso acá estamos mostrando los clasificados a velocidad máxima. Los que están abajo son los que están por debajo de la velocidad máxima en el eje inferior, en el eje X.

Cuando hice esta diapositiva con este gráfico, no había terminado el análisis de los datos, pero noté una tendencia interesante como el pico a la izquierda y ese especie de codo en el medio que desaparece cuando termina el gráfico, cuando terminé los gráficos.

Hay una conducta de rampa descendente. Quiero marcarles los puntos que representan la velocidad mínima que están por debajo. Está este patrón de muchas consultas y después esta desaparición aleatoria. Yo le consulté a mi fuente de datos y todos estos gráficos son de la segunda mitad del día. ¿Por qué pensé al principio que había un problema con los datos? La primera mitad pensé, debe estar mal, la segunda va a estar bien y recibía lo mismo, entonces sigo sin entender.

Bueno, este era el último de los gráficos. Nuevamente, no tengo ninguna respuesta para este comportamiento aleatorio. Consulté a una de las universidades que brindaba los datos que tenían 8 equipos que a la noche estaban en silencio, pero seguían activas pero solo enviaban pedidos durante el día y hacían muy pocas otras consultas.

Le escribí hace dos días al departamento de sistemas con la expectativa de tener una respuesta hoy para hablar con ustedes pero no la tengo. Estuve con mis contactos pero no han respondido. Bueno, como les decía, todo esto viene de un conjunto de datos de una semana. Queremos divulgar este conjunto de datos para que ustedes también tengan la oportunidad de analizarlo.

Abajo vemos un gráfico del sitio web impact cyber trans que usa esta información para fines comerciales. Voy a hablar con la organización de la ICANN para ver si les interesa este conjunto de datos, imagino que sí.

Como decía entonces, la semana va del 9 al 16 de enero y hay varios componentes interesantes. No solo el hecho de que está centrado en la parte de la revocación de la KSK, sino también que en el gráfico inferior, ese gráfico representa un solo día.

Vemos que hay picos en los datos en el número de paquetes recibidos. Son gráficos del sistema de monitoreo. La línea

inferior es el tráfico velocidad normal y esas oscilaciones es alguien que consulta de las direcciones IP de Amazon que son dos o tres veces más grades que el tráfico de consultas. No sabemos por qué hacen esto. Hemos hablado con otros operadores raíz y parece ser que por una cuestión singular se están focalizando en nosotros, tengo que investigar más.

No sé qué está pasando y las consultas que ellos envían son basura. Es como basura alfa numérica, así que si alguien quiere investigar estos datos, por favor pónganse en contacto conmigo y lo coordinaremos.

Pareciera que hay nombres de DNS, algunos codificados en bytes 64 pero es un paquete que yo no entiendo. La verdad que hoy tampoco he tenido mucho tiempo para analizarlo, me gustaría que algún otro también lo analizara y me cuenta. Si podemos atribuir esto al dueño de Amazon que envía todo este tráfico, porque esto está sucediendo desde noviembre, en un patrón semanal está pasando. Y yo contacté a Amazon y me dijeron: “No sabemos quién lo hace”. ¿Cómo no lo saben? Bueno, y hemos usado dos canales de Amazon y bueno, no he tenido respuesta. Queremos saber qué está pasando.

Quería saber si ustedes tienen preguntas. Yo tengo muchas preguntas pero no tengo respuestas. O sea, que quiero saber si ustedes tienen preguntas que yo pueda responder.

JACQUES LATOUR: Gracias, Wes. Parece que hay una filtración a través del DNS. Si le parece usted puede armar todo esto y compartirlo.

WES HARDAKER: Un aspecto irónico es que se habló de que la organización debiera recopilar todos estos datos alrededor de la OARC. La respuesta fue que, "No, esto va a ser muy aburrido".

JACQUES LATOUR: Tenemos 10 minutos para preguntas para todos los panelistas.

EDUARDO DUARTE: Eduardo Duarte de Duane. En la primera animación usted habló del comportamiento de IPv6 pero no se refirió al segundo. Parecía que había oposición entre ambos.

DUANE WESSELS: Las ramificaciones del KSK eran adyacentes a los eventos de la clave. ¿Y usted pregunta o dice que había oposición en todos los gráficos?

EDUARDO DUARTE: ¿En el segundo era antes?

DUANE WESSELS: Depende de la respuesta de la DNS KEY y cuantos registros hay en la zona. En el traspaso añadimos firmas para que la revocación pudiera añadir la clave nueva. Cada vez que hay una respuesta de 12 80 aumenta al doble el tráfico.

[CASSIE]: Esta pegunta es para Wes de Geoff Houston. ¿Hasta qué punto ve la truncación de las respuestas UDP y los problemas posteriores con TCP?

WES HARDAKER: Gracias, Geoff. ¿Puede aclarar? Esto lo hablamos hace un tiempo y no me parece que lo que usted diga sea hace dos o tres años y no es así según nuestra práctica operativa. ¿Lo midió recientemente?

No obstante, puede ir respondiendo. No me parece que haya un gran cambio entre UDP y TCP como lo sugiere el gráfico, me parece que no es así. Tengo que ver en el par de días.

[CASSIE]: Geoff responde, no, no lo medimos recientemente.

WES HARDAKER: Sí, lo medimos. Hace un año tuvimos un comentario similar en un foro parecido y le dije que no, que lo medimos recientemente. Podemos verificar que este problema ha sido resuelto, pero antes del traspaso de la clave hicimos un cambio para que esto no causara problemas.

[CASSIE]: Geoff también dice: "A y J también dice que hay un cambio en el de 1280 bytes".

JACQUES LATOUR: ¿Cuál es la próxima fase para remover?

DUANE WESSELS: El 22 de marzo va a dejar de estar publicado en la zona.

WES HARDAKER: Estos gráficos, los violeta y los verde los hice el 7 de marzo. Son posteriores porque quería ver si el problema había desaparecido y, por supuesto, no desapareció.

JACQUES LATOUR: Fred.

FREDERICO NEVES: Para Duane. ¿Usted contactó a algunos de estas entidades que hacen la mayor cantidad de consultas?

DUANE WESSELS: No personalmente, pero otro operador de servidor raíz está en contacto con las fuentes que más consultas y direcciones hacen. Me encantaría tener una explicación de lo que está pasando. En mi experiencia estas cosas pasan que repentinamente desaparecen y nunca tenemos una explicación.

FREDERICO NEVES: De todas maneras los gráficos son muy buenos.

DUANE WESSELS: Mucho tráfico continúa y tenemos que ser más agresivos a la hora de contactar a la gente y estar alertas. Estén alertas a ver si les damos una respuesta para hacer el seguimiento de las fuentes de datos. A ver si entendemos o podemos determinar qué es lo que realmente está ocurriendo aquí.

RUSS MUNDY: Duane, yo tengo una pregunta para usted. ¿Han considerado proyectar a futuro lo que representaría este crecimiento del tráfico dentro de seis meses, dentro de un año si esto continúa?

DUANE WESSELS: Debo ser honesto y la verdad es que no, pero sería una situación bastante terrorífica. Si calculo bien, estas consultas del DNS aquí son el 6% del total del tráfico que vale la pena tenerlo en cuenta.

JACQUES LATOUR: ¿Alguna otra pregunta?

WES HARDAKER: Un comentario final porque me han escrito… Bueno no, me hubiera gustado, pero dicen que gran parte de esto viene del DigitalOcean, de Amazon, AT&T. Son consultas genéricas, o sea, no sé si ayuda mucho. Van rotando genéricamente.

JACQUES LATOUR: Muy bien. Gracias, Wes.

Kathy, ¿puede darnos las instrucciones para el almuerzo?

KATHY: Sí, el almuerzo es en la sala de enfrente, así que no hay que caminar mucho y les…

[FIN DE LA TRANSCRIPCIÓN]