SINGAPUR – Taller de At-Large: TOR y mecanismos alternativos de nomenclatura para el DNS
Lunes, 24 de marzo de 2014 – 17:00 a 18:00
ICANN – Singapur, Singapur

EVAN LEIBOVITCH: Buenos días a todos. Y buenos días para algunos que sé que es muy temprano en algunos lugares, también sé que para otros es muy tarde.

Y básicamente tampoco me quiero interponer entre esta sesión y la sala, pero vamos a tratar un tema que es muy importante. Por cierto, mi nombre es Evan Leibovitch, soy el Vicepresidente de ALAC, me ubico en Toronto y soy el que estará encargado de esta sesión en el día de hoy.

Cuando comenzamos a habar de los gTLDs y los nombres de dominios y este tipo de cuestiones, a veces la gente dentro de la ICANN se sorprendía y había diferentes enfoques que permitían que la gente pudiera obtener la información que necesitaba en internet.

Esta sesión tiene como objetivo dar una introducción a esto, tenemos hoy dos oradores invitados, en primer lugar Patrik Falstrom que no pudo asistir porque hoy es un día muy ocupado e incluso ha habido hasta (…) dos y tres veces, pero me alegra ver que Joseph si ha podido venir aquí para poder informarnos para que no lo tenga que hacer yo.

Así que sin más que decir, no tenemos diapositivas para esta presentación, en realidad tenemos dos presentadores, y tenemos diapositivas para la segunda presentación.

En primer lugar, a modo de introducción, hablando para Norteamérica que es allá de noche, le quiero agradecer a Dev, Dev Piscitello que es Vicepresidente de Seguridad y Coordinación de TICs para la ICANN.

El nos va a dar una presentación, una introducción, y también algo de contexto respecto de los conceptos subyacen en este tema.

Dev. Adelante por favor. No hay presentaciones, así que ya simplemente lo escuchamos. Adelante Dev.

DEV PISCITELLO: Gracias Evan. Espero que todos me escuchen.

EVAN LEIBOVITCH: Lo escuchamos bien, adelante.

DEV PISCITELLO: A ver. Permítame comenzar diciendo lo siguiente.

Que tuve que cambiar esta presentación dos veces, incluso durante la noche. Lo que me gustaría intentar hacer es comenzar con una descripción de algunas nuevas alternativas y luego volver a la situación del 2006 y hablar de lo que el SSAC había considerado en aquel momento al momento de trabajar con los servicios y los nombres en aquel entonces.

Y también me gustaría tratar o presentar algunas preguntas sobre las cuales pueden pensar y luego quizás, dado que somos dos presentadores solos, podamos también tener lugar para responder las preguntas sin tomar tiempo del tiempo dedicado a la gala.

Quizás tengan preguntas o quizás quieran extender las conversaciones.

Creo que la forma más sencilla de comenzar es asegurarnos de que todos comprendan el concepto de espacio de nombres que es algo bastante sencillo. Es un nombre que se da en un contexto en particular, todos estamos acostumbrados al DNS público, y el espacio de nombres de dominio que les permite a las personas asignar nombres y utilizar nombres que son bastante más amigables o familiares que un número e identificar esto con páginas web, servidores, wiki, etc. etc.

Una de las necesidades por las cuales es necesario tener espacios de nombres, entre otras, es que existen administradores globales de los identificadores en el espacio de nombres.

Tener una Gobernanza global de esto siempre es un desafío. No necesariamente históricamente ha habido muchos espacios y no siempre todo el mundo está contento, esto se nos lleva a los ’70 o a los ’80 cuando teníamos un sistema operativo o teníamos determinados sistemas operativos como el SNE, DEVNET o SXNS y otros nombres de espacios y en algunos casos no eran necesariamente utilizados pero, había algunos criterios establecidos respecto de cómo utilizar nombres en distintos escenarios de trabajo.

Cuando comenzamos a utilizar el DNS, allá por los ’90, los ’80, teníamos nombres de espacios de dominio, nombres de espacios, que estaban asignados a los dominios de alto nivel que ahora se denominan genéricos. Y eso comenzó a identificar nombres de espacios que son utilizados por los países individuales que se denominan también ccTLDs. Y para fines de los ’90 y a principio de 2000, la gente podía tener acceso

a los nombres de dominio de alto nivel con una serie de nombres expandidos en la raíz.

Esto apareció también en forma de nuevos gTLDs a mediados de los 2000.

Durante todo este tiempo, en realidad en el 2006, yo informaba al SSAC, SSAC 009, ese informe habla de los servicios de nombres de dominio y de la raíz. Es uno de los casos en los que creo, el SSAC consideró la noción de por qué la gente en realidad quería tener nuevos espacios más allá del DNS público y esto tiene que ver con la colisión de nombres, o lo que yo prefiero llamar la superposición de espacios de nombres de dominios.

Algunos de los problemas que se están tratando de resolver cuando hablamos de los espacios de nombres de dominio alternativos o estamos tratando de cambiar el control actual y esa responsabilidad de controlador ahora, como mencionó Fadi, ha pasado a nosotros.

Esto ha sido así desde el 2006 y tenemos en algunos casos, alternativas comerciales y otras también tenemos sistemas o TLDs que tienen motivaciones políticas por ejemplo.

Hace algunos años, unos nueve años atrás, la motivación quizás era distinta, pero básicamente era igualmente importante.

Otra razón por la cual quieran tener un nombre de espacio de dominio hoy es para administrar lo que se llama las licencias para discutir las colisiones de nombres, porque hay gente que quiere continuar haciendo lo que está haciendo, como por ejemplo tener TLDs, o crear etiquetas en nombres privados o espacios de nombres privados, es decir, esto puede

lleva a una superposición de nombres de espacios o también solicitar un dominio de alto nivel.

Entonces surgen algunos problemas que quizás se deseen resolver. Mientras escuchaba a Garth y a los que hablaron después, uno debe pensar qué es lo que se debe tratar de resolver.

Y también pensar cuáles son las consecuencias y cuáles son los beneficios.

En algunos casos cuando considerábamos este problema en 2006 la alternativa era una.

En algunos casos había que hacer sacrificios, por ejemplo había que decidir tratar de utilizar nombres de espacios que no tuvieran ningún problema en los buscadores, lo cual era muy extraño.

Y que pueden existir cuando uno comienza a crear nombre de espacio de dominio y los empieza a balcanizar.

Y esto también pasándolo a varios espacios.

Entonces, cuando un piensa qué es lo que va a sacrificar, qué es lo que va a inventar también tiene que medir cuáles son las consecuencias, qué es tolerable.

Otro aspecto sumamente importante es considera algo que tiene que ver con el DNS público, si se va a hacer algo, bueno, entonces cómo se va a afectar. Hay que identificar las consecuencias que se puede tener si es que uno por ejemplo no puede controlar o hacer separaciones de espacios de nombres entre organizaciones.

Otra suposición, que quizás puedan tener en cuenta, es qué protección se busca o se utiliza para los TOR que desde algún punto de vista tienen otras razones para existir y que son alternativas. Por ejemplo, podemos hablar de esto luego.

Lo último que quiero mencionar es que ya que yo pertenezco al equipo de Seguridad y estamos preocupados sobre el DNS y el uso que tiene este DNS por parte de los delincuentes. Hay muchos abusos y también políticas implementadas al respecto. Pero tenemos que identificar cuál es el problema ahora.

Garth ya habló de otro problema que también hay que prestarle atención y ¿estamos preocupados de los ataques al DNS cuando el DNS genera un problema?

Entonces – y esto se traslada a otros usuarios u a otras aplicaciones en internet – esto ya no va a ser invisible.

Entonces, es críticamente importante en la forma en que nosotros utilizamos internet.

Hace unos treinta años internet -no teníamos DNS, no teníamos buscadores, no teníamos muchas cosas. Entonces para poder trabajar había otras cuestiones que teníamos que tener en cuenta. En el futuro mucho del DNS va a cobrar más importancia. Entonces tenemos que considerar estas cuestiones.

Pero son cosas que debemos analizar conforme avanzamos con nuestros debates.

Y ahora le voy a ceder la palabra a Garth.

GARTH BRUEN: Bueno. Gracias. Habla Garth Bruen. Soy Presidente de la región del Ralo de América del Norte. Y estoy aquí trabajando en representación de At-Large en cuanto a cuestiones de Cumplimiento.

ORADOR NO IDENTIFICADO: ¿Garth tiene diapositivas para nosotros verdad?

GARTH BRUEN: Gissela por favor si pudiéramos pasar a la primera diapositiva que tiene un signo de pregunta. Porque ya hemos cubierto algunos de los puntos básicos.

Una más por favor. Gracias.

Soy Garth Bruen Presidente de NARALO. Y yo pedí esta sesión. Una de las razones era porque esta discusión no se estaba llevando a cabo, y la razón por la cual no se estaba levando a cabo en general es porque las estructuras de las que estamos hablando hoy no son operativamente o contractualmente parte de la ICANN.

Y también hay otras razones por las cuales esto tenía que aparecer en una reunión en la ICANN.

Me parece que es importante que hablemos de esto porque están allí y no vamos a hacer juicios en esta discusión de que si son buenas, pero bueno, tenemos que poner los hechos sobre la mesa.

Siguiente diapositiva por favor.

Bien. Tenemos que poder crear políticas, tenemos que poder tomar decisiones que sean informadas.

Uno de los hechos que tenemos que tomar en cuenta es la toma de decisiones y que también hay muchos sistemas de nombres que existen. Si la ICANN quiere llegar a todos tenemos que preguntarnos por qué estos sistemas alternativos son requeridos o son necesarios.

Algunos piensan que son una amenaza, otros piensan que hay que ignorarlos directamente y otros piensan que hay que tenerlos en cuenta y debatir al respecto.

Esto conceptualmente es que el DNS que es el foco principal de las sesiones de la ICANN no es toda la internet, sino que es una muy pequeña parte. El espacio de IP es la parte más importante. Sino que hay una parte habilitada del DNS que tiene contenido. Pero es una porción muy pequeña.

Entonces ¿qué es lo que sucede en el resto de este espacio que no tiene nombres de dominio?

Bueno. Es muy interesante saber qué es lo que sucede en esta partecita.

Hay tres tópicos importantes. Son los dominios sin nombres, entre otros

Ahora. En cuanto a los TLDs o raíces alternativas. Hay más de 400 TLDs que no son de la ICANN que están operando, posiblemente haya más. Hay algunos que están en documentos y hay otros que no están documentados para nada.

Y lo que quiero decir con esto es que estos son los que se han publicados y han sido descubiertos por una u otra razón.

Por ejemplo, dos personas o un grupo de personas pueden crear su propio TLD, tener su propio protocolo para hablar entre sí y nadie se tiene por qué enterar de esto.

Algunos ejemplos podrían ser, la raíz siriana, que tiene más de 100 TLDs, el espacio ".nombre" o "space.name" que tiene más de 90 TLDs, NewNet que hizo juicio a la ICANN, pero no conozco cuál es el estado de ese juicio. Luego tenemos NewNations de OpenNIC, y también hay otros que no se han identificado, como por ejemplo (inaudible) entre otros.

¿Por qué existen estos espacios alternativos?

Existen diferentes razones para esto.

".espacio" bueno, ellos no piensan que la ICANN cumpla con el público o le sirva al público, entonces quisiera crear su propio espacio.

SIRIO tiene independencia política, es una entidad soberana que quiso tener su propio espacio de dominio y no confiar en nadie.

".bit" es parte de un experimento económico y tiene que ver o se utiliza en la arquitectura de pago de "bit coin" que es una moneda virtual, y luego, tenemos ejemplos como ". jack", que fue creado por un caballero que estaba preocupado por las raíces alternativas. Decía que las raíces alternativas eran malas, entonces él decidió crear su propio espacio.

Luego tenemos otro ejemplo como ".pirata", que fue creado –como ya se lo pueden imaginar – hacer transferencias ilícitas, bajar material, etc.etc.

El SSAC aborda algo muy específico que son los dominios sin punto.

¿Qué es un dominio sin punto? Bueno. Exactamente lo que parece que son.

Es un dominio que no tiene una extensión de TLD.

Hay gente que dice “bueno, pero esto es imposible, cómo un nombre de dominio puede no tener un punto”.

Bueno Es simplemente muy sencillo, es un nombre que está adjuntado a una dirección de IP y no necesita un punto.

El ARPANET originalmente no tenía ningún punto, los nombres de “host” existían antes de que los nombres de dominio con punto aparecieran.

Los dominios TOR, que aparecen entre comillas, porque no siempre tienen el TOR, es en realidad un DNS según nuestro entendimiento del DNS – sin embargo el sistema toma en cuenta identificadores únicos que se refieren como nombres de dominios, pero estos nombres no pueden llegar al nombre de dominios. Entonces también se los denomina “servicios ocultos” o TOR. Y por ejemplo sería el “.onion” o “.cebolla”.

El sistema no los toma en cuenta.

Siguiente diapositiva por favor.

Sin embargo, vamos a hablar del TOR porque el TOR no es primariamente para los nombres. El sistema TOR agrega capas de ruteo para oscurecer el tráfico y también hay cierta protección y esto va en contra a como debería funcionar la internet. La internet que conocemos, el traspaso de información y direcciones son cortas y el traspaso es claro. Aquí no.

Esto es básicamente un cuadro que muestra cómo funciona el TOR, se extrajo de la documentación de TOR, donde se crean raíces arbitrariamente mucho más largas para dar oscuridad a los puntos de intercambio existentes en todo el proceso.

Como pueden imaginar, puede ser un tanto lento. Así que la gente que utiliza lo hace a una velocidad determinada para evitar que sean descubiertos.

Siguiente diapositiva.

También hay una pregunta que dice si el TOR es únicamente para los delincuentes o para los mercados negros. Básicamente es para esto. Y esto ha llamado la atención de muchos de los medios y es un gran, gran tema.

Sin embargo, en lo que sucede aquí, bueno, no refleja lo que hace la comunidad de TOR y esto también se aplica al DNS.

¿Quiénes utilizan el TOR?

Bueno. El TOR es utilizado por agencias de cumplimiento de la ley, activistas, periodistas, es decir, cualquiera que quiera proteger su identidad.

Siguiente diapositiva, por favor.

Me reuní con representantes del Proyecto TOR y bueno, les pregunté qué era lo que querían que la gente supiera y qué era que la gente se olvide.

Y ellos me dijeron que querían que la gente se diera cuenta o supiera que TOR es una comunidad formada por personas que mantienen el software y mantienen sus redes. Esto no tiene como objetivo remplazar el DNS, lo que se está tratando de hacer es brindar seguridad a personas que necesitan seguridad, porque hay muchas personas que necesitan seguridad por diferentes razones.

Esto es un pantallazo general muy breve, porque es un tema muy complejo.

Hay una serie de cuestiones, una serie de problemas.

Tenemos confusión de los consumidores, y las colisiones, estos son temas bastante cerrados porque hay gTLDs o nombres de dominios que son muy similares.

Uno tiene que ver cuando el usuario tiene el problema y en el segundo caso es cuando hay un tema técnico.

Luego tenemos las cuestiones legales. En este espacio hay muchas cuestiones judiciales involucradas. Especialmente cuando se tiene un sistema alternativo que tiene su propio sistema TLDs y se dice o acusa a la ICANN de violar ciertas reglas.

También tenemos cuestiones de seguridad, y como saben también tenemos la cuestión que debatimos constantemente que es el de la gobernanza.

Hay fortalezas y debilidades en los sistemas alternativos.

Con algunos de estos sistemas alternativos no hay intercambio de dinero, es decir que el acceso a estos dominio sea gratuito.

Pero esto no se aplica para todos los sistemas alternativos. En algunos de estos sistemas no hay titulares de registros, no hay personas que se preocupen por esas cuestiones. Pero también estos sistemas han establecido sus propios sistemas de WHOIS y recaban datos.

Y luego también tenemos la cuestión de la responsabilidad, cuestiones de la flexibilidad de estas redes cuando se las utiliza, y también tenemos preguntas o cuestiones que tienen que ver con la seguridad.

Es decir, son problemas complejos en todas estas áreas que están fuera del DNS regular, pero también tienen este foro para poder reunirse y discutir, cosa que pueden no existir en otros sistemas.

Lo que hemos venido escuchando desde hace un tiempo es “un mundo, una internet” ¿podemos realmente decir esto aquí?

Estas en realidad son preguntas para disparar la reflexión. Si fuera necesario por algún motivo imprevisto de tener un sistema alternativo ¿sería esto posible?

¿Conceptualmente los sistemas alternativos son una innovación o una imitación?

Y una pregunta en general para los dominios como concepto.

¿Van a ser válidos dentro de 10 años? ¿Van a ser remplazados por una nueva capa u otra cosa que funcionará mejor para el usuario final?

Esto entonces dejará de ser un problema.

Y bueno, con esto quisiera abrir el debate, escuchar otras ideas y a otras personas.

Gracias.

EVAN LEIBOVITCH: Gracias Garth. Entramos ahora en la sesión de preguntas y repuestas. Les pido por favor que se identifiquen antes de hablar que hablen despacio.

Creo que sigue el servicio de interpretación en varios idiomas. Y eso significa que si ustedes desean hacer uso de la palabra, en chino, en francés o en español lo pueden hacer. Hay auriculares en la entrada de la sala, si ustedes los necesitan.

Voy a empezar con una pregunta mía, personal, antes de abrir a la mesa.

Una cosa que me gustaría que cualquiera de los dos o cualquiera de los presentes es que analice el tema de la accesibilidad.

Varios de los nuevos gTLDs tienen problemas de acceso por los navegadores.

¿Qué impedimentos representan estos sistemas alternativos?

¿Se requiere un “plagging” para el navegador o hay más dificultades de uso?

GARTH BRUEN: Rápidamente. Algunos requieren configuraciones propias o incluso software. Pero algunos de los paquetes alternativos, si, permiten acceso a todos los materiales.

Es interesante, pero es un tema que necesita más exploración, más análisis.

DAVE PISCITELLO: Evan no me queda claro. Hace unos años –

EVAN LEIBOVITCH: Se entrecorta el audio.

DAVE PISCITELLO: Una de las cosas que descubrimos hace varios años es que la forma en que la mayoría de los sistemas todavía funcionan con el DNS, es que requieren cierta pre-configuración. O algún tipo de consulta que les dé un indicio de dónde comienza el DNS.

En todos los casos que yo analicé y creo que sigue siendo así, no tenemos muchas de estas rutas alternativas que tienen los sistemas operativos comerciales que disfruta la IANA, en el sentido de que hay coordinación entre los sistemas operativos para iniciar correctamente el espacio de nombres.

EVAN LEIBOVITCH: Tenemos varios pedidos de uso de palabra. Alan primero.

ALAN GREENBERG: Dos comentarios. Primero, con respecto a lo que preguntó Garth, esa pregunta de qué vamos a tener dentro de cinco o diez años, si el sistema actual de DNS será incluso relevante.

Bueno. Hay un período de larga data de estacionamiento de la tecnología, con algunas excepciones. El tiempo que lleva desde que se demuestra algo en un laboratorio hasta que se convierte en algo ampliamente aceptado, suele ser de ocho años.

Hay algunos casos ocasionales en que son más rápidos, pero no muchos casos.

Eso significa que cuando uno intenta predecir qué será lo que estará de moda dentro de diez años, el desafío es grande.

No voy a animarme a decir qué será el remplazo del sistema DNS dentro de unos años o cuál será el sistema implementado.

El mundo es demasiado complejo, hay demasiadas variables como para poder predecir.

No hay que ir a hablar de TOR para reconocer que hay cosas que hacen enrutamiento propio y que tienen sus propios sistemas de búsqueda. Skype en especial, al comienzo, después de que lo tomó Microsoft, para funcionar en dispositivos móviles, era un mundo que funcionaba autónomamente.

Si uno tenía una computadora con múltiples conexiones a distintas redes, Skype seguramente habrá usado el nodo ajeno para saltar de una red a la otra y decidir cuál era el mejor lugar de destino, y por eso tenía su propio sistema de nombres completamente externo a lo que es el DNS.

Es algo muy común que todos usamos, pero que no representa una amenaza.

Hay muchas coas en este mundo que son potencialmente peligrosas y si quisiéramos construir nuestro propio sistema Skype y dejar de usar el DNS, sería un sistema muy complejo pero podría usarse y podría funcionar.

DAVE PISCITELLO: Yo creo que cuando vemos como se usaban los nombres de dominios a finales de los ’90 y cómo usamos ahora los dispositivos móviles con búsquedas habilitadas por voz, o búsquedas por otros medios cliqueando simplemente en un icono en un dispositivo móvil, para conseguir lo que queremos sin tener que preocuparnos cuál es el nombre de dominio. Eso nos permite argumentar que ya tenemos un espacio alternativo.

El motor de búsqueda utilizar el lenguaje natural. Y la importancia, por así decir, de un nombre de dominio es que funcione – por ejemplo en el caso de una marca – funciona mucho mejor hoy día en un dispositivo móvil que lo que hacía en una PC a finales del ’90.

Reconozco como se dijo, que hay una evolución y tenemos que reconocer que hay cambios en el mercado de lo que es un nombre de dominio.

Si pensamos en la infraestructura de la internet actual, pensamos en el caso de un plomero. El plomero no confunde el caño de fluentes o del sistema de aguas servidas con el de agua potable. La internet tampoco.

Si la discusión de si los nombres de dominio van a importar o no, creo que sería mejor verlo desde el punto de vista siguiente. A medida que

los nombres de dominio importen menos porque van a estar más embebidos y serán más invisibles para el usuario.

¿Cuál sería la forma más eficiente de habilitar el acceso a los recursos que estamos buscando en internet? ¿Y qué rol jugará ICANN o qué rol jugará la comunidad de múltiples partes interesadas en la administración de ese nuevo espacio?

EVAN LEIBOVITCH: Ok. ¿Quién sigue? Eduardo.

EDUARDO DIAZ: Gracias. Soy Eduardo para la transcripción. Tengo una pregunta sobre la red TOR y cómo se relaciona esto con lo que hemos escuchado hablar de que el DNS hace espionaje en internet.

¿TOR puede espiar? ¿La red ".tor" puede espiar?

GARTH BRUEN: Perdón. Estaba hablando remotamente por el chat. Te pido por favor que repitas la pregunta.

EDUARDO DIAZ: Básicamente lo que decía que es con estas noticas de que se espiaba internet por DNS? ¿Aquí, también se incluía la red TOR?

GARTH BRUEN: Bueno. Eso incluiría absolutamente todo. Es una historia compleja porque el Gobierno estadounidense estuvo involucrado en la creación

de TOR. Se creó en el laboratorio de la Armada estadounidense. Y fue usado por varios organismos gubernamentales en todo el mundo.

Creo que Alan tiene una respuesta específica al respecto.

ALAN GREENBERG: Si. Dos partes. Recientemente descubrí, recuerdo una discusión que tuve con un ingeniero senior en redes, en el año 1995, o sea hace muchos años. Hablábamos de lo que era en esa época los “hard” centrales MAE West, y cada uno tenía un gran cable y una sala al lado que se usaba para capturar todo el tráfico para el Gobierno. Esto entonces no es exactamente novedoso.

Respondiendo específicamente a la pregunta. Corre por la red IP, es visible en los enrutadores el HAD Central. La única pregunta es hasta qué punto se puede reconocer el tráfico y decodificarlo o (desencriptarlo).

Probablemente las chances de que puedan hacer son muchas.

NIELS TEN OWVER: Creo que tenemos que ser más precisos a la hora de hablar de TOR.

Ha habido unas diapositivas muy explícitas de la NSA que muestran que no se puede filtrar el tráfico de TOR.

Han habido implantes de versiones antiguas de Firefox para hacer “upstream” tratando de focalizar o llegar a usuarios de TOR, pero este no fue un grupo muy grande. Y antes de que saliera el “patch”, el día cero, ya estaba el parche del equipo de TOR.

La diapositiva de la NSA decía que para ellos es prácticamente imposible quebrar el TOR.

Está la opción teórica de hacer un ataque sincronizado donde la NSA filtraría toda la red y por correlación sincronizada del ataque, ver de dónde viene el tráfico y así identificar al usuario. Pero para eso tendrían que monitorear toda la red en tiempo casi real. Y bueno, no pensamos que tengan la capacidad por lo menos todavía.

Entonces creo que debiéramos decir que si uno quiere ser anónimo en la red la mejor opción es TOR.

EVAN LEIBOVITCH: Habiendo dicho esto ¿debiéramos nosotros tener en cuenta el hecho de que ha habido oportunidades en el pasado donde la NSA nos ha dicho que no han hecho cosas que en realidad si hicieron?

Entiendo lo que usted dice, el hecho de que la NSA tenga una diapositiva que diga que no pueden hacer una cosa, no necesariamente va a hacer que yo lo crea.

NIELS TEN OEVER: Bueno. La NSA de hecho no lo dijo. Nosotros lo averiguamos y se filtró.

Fue una reacción a lo que se dijo del dinero que iba a TOR o que se usó para el desarrollo en los laboratorios de la Armada, lo desarrolló Dingledine con fondos que fueron utilizados por los militares.

Siempre ha sido código abierto, y basado en protocolos criptográficos de mejores prácticas.

No quise insinuar algo que no era.

DAVE PISCITELLO: No quiero estar en desacuerdo con lo que la NSA puede (desencriptar) o no. Pero quiero decir que TOR es utilizado por organismos de vigilancia, lo usan los criminales, los periodistas, personas que necesitan libertad de expresión.

En agosto del año pasado el FBI entró a la red TOR encubiertamente en un caso de abuso de menores.

Hay varias coas aquí cuando hablamos de la vigilancia de TOR.

Quebrar el encriptado de TOR es una cosa y poder entrar a la red de TOR es otra.

Como es anónima no hay un proceso activo en la red TOR que permita bloquear activamente los agentes de vigilancias, ya sean de Gobiernos u otras partes. Uno es anónimo pero también son los demás, y el tráfico está encriptado. Es un desafío (desencriptar) algo aisladamente.

Por otra parte TOR es barato, es muy accesible y la NSA no es la única agencia del mundo que recurre a TOR.

Correr muchas máquinas en paralelo, tomar la encriptación de un mes o de un año; en teoría podría ser algo práctico aún cuando en la práctica por lo menos no lo es.

EVAN LEIBOVITCH: Gracias Dave. La siguiente pregunta viene de un señor que levantó la mano.

Tiene la palabra, por favor identifíquese.

WARREN KUMARI: Soy Warren Kumari. Llegué tarde así que si el tema que voy a preguntar se trató, les pido que me interrumpan.

La posibilidad de filtrar o de hacer una fuga de la información a través de la DNS, seguramente, ustedes han escuchado hablar de casos así. Hay un proyecto, un borrador que hemos escrito con Andrew Sullivan en el IETF que analiza formas de mitigar las fugas de información, en general cuando la gente utiliza nombres similares a los que se utilizan en el espacio de nombres.

Aquellos separados con puntos. Cuando se usa esto en contexto no DNS sugerimos que se reserve una etiqueta para denotar que es un espacio de nombres alternativo.

Entonces básicamente si se está utilizando un esquema de nombres alternativos se agrega una etiqueta al final para indicar que esto es distinto de un nombre utilizado en el contexto de DNS.

Este proyecto es wwwcamari.tld, creo que ese es el nombre.

EVAN LEIBOVITCH: Le pido por favor que si usted tiene acceso a adobe connect lo (tipee) en el chat, así aquellos que están interesados lo pueden conocer.

Bueno. Luego tengo a Garth y una pregunta del chat.

¡Garth!

GARTH BRUEN: Gracias. Quería volver a un comentario que se hizo anteriormente respecto de la seguridad de TOR. Una pregunta que hizo el colega.

¿Hay alguna preocupación sobre la seguridad de los nodos de salida? ¿Los “exit nodes”?

Ha habido varias publicaciones, publicaciones teóricas y también investigaciones realizadas, acerca de nodos de salidas posiblemente comprometidos. En el modelo de amenazas que se mostró, se ve claramente que el tráfico dentro de la red TOR está encriptado entre los nodos. Pero no está encriptado desde el nodo de salida hasta el tráfico final.

Entonces, de hecho es posible que los organismos de aplicación de la ley u otras pates interesadas o terceros puedan acceder a los nodos de salida y así capturar el tráfico.

Pero esto sería aun así, bastante difícil, sería difícil saber a dónde va a tráfico o a quién va el tráfico. Podría ser entonces posible tener una cierta idea del tráfico pero no vincularlo con el punto de origen.

Por eso se usa los “exploits” de navegadores y otras adiciones.

Entonces sí, es una preocupación pero no necesariamente un preocupación generalizada.

GARTH BRUEN: Para que todos entiendan, en la red TOR de punta a punta no sabemos con quién estamos hablando ni sabemos dónde están, pero la persona inmediatamente delante nuestro si sabe que es el operador del nodo de salida.

¿Dave tienes algo que agregar?

DAVE PISCITELLO: No. Creo que está bastante claro lo que se dice acerca de la función de TOR.

EVAN LEIBOVITCH: El que sigue es Gisella Gruber quien va leer comentarios del chat de adobe connect.

GISELLA GRUBER: Tenemos una pregunta de Poomjit net…….

Me gustaría saber qué aplicación es más segura para los usuarios –que aplicación de “chat room”- es más segura, en especial para activistas que tienen que trabajar y vivir en crisis políticas tensas.

EVAN LEIBOVITCH: No estoy seguro si esto se aplica a nuestro tema, pero bueno, si alguno de ustedes quiere formular alguna recomendación rápida, la pondríamos en el “chat room” para que nuestro amigo sepa la respuesta.

Yo tengo mis propias recomendaciones acerca de cuáles son los chat romos más seguros, pero seguramente cada uno los tiene.

Sería mejor entonces que si alguno tiene alguna recomendación lo ponga en el chat para ayudar al colega.

¿Hay alguna otra pregunta?

Tenemos personas muy calificadas aquí en la mesa. Este es entonces el momento para hacer preguntas.

Quería agregar un comentario de mi parte que es recordarle a la gente que hay un grupo de trabajo sobre métricas de gTLDs que se ha creado para aumentar la confianza de los consumidores, que comenzó con el Programa de nuevos gTLDs y una de las cosas que ha intentado hacer el ALAC es asegurar que las métricas no necesariamente digan, bueno, está bien que ahora tengamos más opciones gracias a que tenemos un par de cientos de nuevos gTLDs. Sino también asegurarnos de que las métricas también midan la popularidad del DNS relacionado con las alternativas.

Con la posibilidad de que si hay confusión de los consumidores por este masivo influjo de TLDs ¿Esto va a hacer que la gente se vaya a los alternativos, se vaya a TOR, se vaya a aplicaciones móviles, a páginas de medios sociales, etc.?

Bueno, eso es algo simplemente a tener en cuenta a la hora de analizar los sistemas alternativos. Se dan cuenta de la edad que tengo porque hablo de cosas como la CPU, el uso de ".onion", me recuerda lo que era el ".ucp", ese pseudo-dominio.

¿Garth tenías algo que agregar?

GARTH BRUEN: Creo que – o espero que podamos tener esta estructura o mantener esta estructura a lo largo de las diferentes estructuras de la ICANN para poder continuar con estos debates específicamente y también quizás podríamos tener algunas reglas para estudiar los DNS alternativos y recabar más información al respecto. Quizás también (inaudible= pudiera publicar esa información.

EVAN LEIBOVITCH: Bueno. Yo como Presidente de la reunión voy a decir que tenemos muchos expertos desde varios puntos de vista aquí. Así que afortunadamente le vamos a pedir a algunos de ustedes que al final se acerquen para que podemos comenzar a trabajar con este grupo de trabajo.

¡Glenn adelante!

GLENN MCKNIGHT: Simplemente quería hacer un comentario respecto de lo que dijo Garth.

Nosotros vamos a estar en el IETF en Toronto en junio pero también estamos organizando un foro en octubre en Canadá.

Esto parece una muy buena discusión, así que me gustaría facilitar de alguna manera una en junio y otra en octubre, así que por favor acérquennos a mí o a Evan para poder avanzar con esta sesión

Gracias.

EVAN LEIBOVITCH: Nos quedan diez minutos y puedo ver que la gente ya se está yendo. Tengo dos preguntas más.

Primero le voy a dar la palabra a Eduardo.

EDUARDO DIAZ: Para los registros. A ver. Me causa curiosidad esto. Ya he usado el TOR antes, si yo uso un buscador de TOR puedo buscar cualquier cosa en internet, pero el tema es que uno no va a saber de dónde bien. Es eso lo que sucede ¿correcto?

Eso es lo que yo tengo entendido.

EVAN LEIBOVITCH: Por favor responda al micrófono porque tenemos gente en la participación remota.

ORADOR NO IDENTIFICADO: Si.

EDUARDO DIAZ: A ver. Quiero que se expanda un poco. Si yo utilizo un buscador en TOR para buscar en internet.

¿Qué es este otro espacio? ¿Cuál es otro espacio alternativo del que estamos hablando? ¿Podemos llegar a otro espacio alternativo a través de un buscador?

GARTH BRUEN: El espacio de internet está en realidad separado del espacio del concepto de TOR. Son otros sistemas alternativos que no se pueden acceder a través del DNS normal. Tienen una configuración especial.

TOR puede ser una de las formas de hacerlo, pero hay otras. El TOR para muchas personas es más bien para la comunicación, se usa para comunicación.

EDUARDO DIAZ: Bueno. Entonces estamos hablando de dos cosas. TOR es una cosa y los espacios alternativos son otras.

Correcto gracias.

GARTH BRUEN: El siguiente orador.

NIELS TEN OEVER: Soy el representante de la NCUC. Tengo dos puntos que pueden ser de interés.

Creo que también hay otras razones para utilizar las direcciones que tienen la extensión ".onion" o cebolla y que tiene que ver con los ataques.

Entonces me parece que esta es una razón para evitarlas y para evitar los ataques.

En segundo lugar, lo que quizás es una de las cuestiones más interesantes respecto de los sistemas de dominios alternativos es cómo

estos interactúan y hay un proyecto – hay que prestarle atención a un proyecto que se llama TOR TO WEB o TOR a la Web, que utiliza un proxy. Quizás aquí se puedan unir o vincular diferentes áreas.

EVAN LEIBOVITCH: ¿Podría por favor colocar ese link que usted está mencionando en la sala de chat del "adobe connect"?

Adelante Dev.

DAVE PISCITELLO: Dos puntos o dos cuestiones. Si van a – quizás quieran considerar esta cuestión mediante el SSAC.

EVAN LEIBOVITCH: Perdón Dave. Usted se está refiriendo a las recomendaciones del SSAC 009 ¿correcto?

DAVE PISCITELLO: Si es correcto. Me parece que esto es interesante, al menos para mí. Es interesante que identifiquemos las diferentes cuestiones y que intentemos o tratemos de identificar cinco clases distintas de nombres de dominios alternativos y que también lo hagamos con los nombres de dominios privados porque también tenemos que tener en cuenta los comerciales, entre otros.

Esto sería una taxonomía interesante de desarrollar y también de rever y ver si pueden surgir nuevas cuestiones y si estas cuestiones se van a abordar.

Este sería un punto.

El segundo punto que me gustaría mencionar es el siguiente.

Cuando hablamos de sistemas de nombres alternativos, mi pregunta o lo que me viene a la mente es ¿Qué estamos dispuestos a sacrificar? Porque el DNS no es únicamente nuestro sistema de operaciones o el que determina cómo operamos nuestras operaciones. Entonces, yo creo que debemos considerar cosas como por ejemplo una revolución en el control, es decir, qué vamos a controlar y qué no.

La otra cuestión tiene que ver con los errores y con la capacidad de resolver nombres o en algunos casos resolver cuestiones que surjan.

Seguramente uno está interesado en controlar determinada información o datos y algunos en ir más allá de ese control.

Creo que esto es importante o el tercer punto es importante para una gran cantidad de personas que tienen que ver con la balcanización universal, básicamente en un escenario de colisión de nombres donde tenemos dominios de alto nivel que son bloqueados o que están en conflictos con otros.

Es decir, son situaciones específicas que se presentan y hay otra cuestión que mencionó Garth, que no debemos olvidar y que tiene que ver con la responsabilidad de la administración o del administrador y la responsabilidad de la transparencia. Eso también debemos tenerlo en cuenta.

EVAN LEIBOVITCH: Muchas gracias a Dave y buenas noches. Garth usted tiene la última palabra.

GARTH BRUEN: Bueno. Muchas gracias. Yo creo que vamos a tener que continuar con esta discusión en próximas reuniones y vamos aquí a terminar.

EVAN LEIBOVITCH: Bueno. Nos faltan tres minutos para llegar a la hora, así que espero que esta sesión les haya resultado informativa, como me resultó a mí.

Nuevamente gracias y que tengan un buen final del día.

[FIN DE LA TRANSCRIPCIÓN]