NATHALIE PEREGRINE: La grabación de esta llamada ya ha comenzado y voy a pasar lista. Buenos días, buenas tardes y buenas noches, a todos, y bienvenidos a la llamada del grupo de trabajo de At-Large sobre tecnología este día 16 de noviembre de 2015.

En la llamada del día de hoy, tenemos a Alexis Anteliz, Harold Arcos, Lutz Donnerhacke, Klaus Stoll, Vernatius Ezeama, Carlos Quintana, Gordon Chillcott, Stuart Clark, Glenn McKnight, Maureen Hilyard, Dev Anand Teelucksingh, Alfredo Calderón, Carlos Watson.

Nuestros oradores invitados en los proyectos [CORE] son David Goulet. Él está al teléfono con nosotros. Bienvenido, David.

Hemos recibido disculpas por parte de Olivier Crepin-Leblond.

Por parte del personal, tenemos a Terri Agnew y a mí, Nathalie Peregrine.

Me gustaría recordarles a todos que hagan el favor de indicar su nombre antes de hablar con fines de transcripción. Muchísimas gracias y le cedo la palabra, Dev.

DEV ANAND TEELUCKSINGH: Muchísimas gracias, Nathalie. Gracias por participar en esta llamada. Sé que algunos de ustedes son tal vez - quizá esta sea su primera llamada al grupo de trabajo sobre tecnología. Así que pensé que me gustaría hacer una breve descripción de lo que se trata el grupo de trabajo At-Large sobre tecnología.

Así que acabo de organizar algunas diapositivas. El grupo de trabajo sobre tecnología evalúa y revisa las Tecnologías de la Información y la Comunicación, TIC, que pueden ayudar a la comunidad At-Large - esas son el ALAC, las RALO, las Estructuras de At-Large - más capaces de cumplir con su papel en las actividades de la ICANN.

Así que cualquier persona interesada en las TIC y en la manera en que pueden aplicarse para resolver las necesidades de At-Large de la ICANN y otras comunidades de la ICANN son bienvenidas a incorporarse al grupo de trabajo sobre tecnología. Lo pueden hacer vía correo electrónico al personal de At-Large de la ICANN, la dirección del correo electrónico es la del personal.

Sólo por nombrar algunas de las actividades [inaudible] hechas entre la ICANN 53 y la ICANN 54, las dos reuniones públicas cara-a-cara de este año, hemos considerado a Kavi como una posible herramienta de proceso administrativo de política como proyecto. Hemos analizado tecnología tal como Teamup, que es un grupo calendario utilizado por difusión y alcance del ALAC y el subcomité de compromiso.

También tuvimos debates acerca de las cuestiones de la lista de correo electrónico de la LACRALO. También tuvimos un debate con las personas de LACNIC para discutir su proceso de desarrollo de políticas, y estudiar sus herramientas. Incluso también le echamos un primer vistazo a la aplicación móvil en beta para la reunión de Dublín de la ICANN.

Sólo para decir que está abierto a todos los miembros de At-Large de todas las cinco regiones de la ICANN - América del Norte, América Latina, el Caribe, África, Asia, Australia, Islas del Pacífico, y Europa.

Sólo para concluir rápidamente, el grupo de trabajo sobre tecnología cuenta con miembros de la comunidad At-Large y otros miembros de los AC y las SO. Ahora tenemos personas del GAC que se unen a este grupo de trabajo. Tenemos una o dos conferencias telefónicas por mes. Hay dos enlaces allí que habla sobre donde se puede encontrar más información. Parte de la documentación que hemos hecho para la comunidad de At-Large en términos de herramientas de traducción y así sucesivamente.

Me gustaría ahora decirles por qué tenemos esta llamada el día de hoy. Esta es una de las recomendaciones de la Cumbre de At-Large. Para los que no saben, la Cumbre de At-Large fue una reunión de todos los representantes de At-Large que tuvo lugar durante la 50va reunión de la ICANN. En esa reunión, todos los representantes de At-Large desarrollados [inaudible] recomendaciones y observaciones. Fueron 43 recomendaciones en total. Lo pueden encontrar en el enlace en la presentación.

Algunas de estas recomendaciones fueron dadas a la TTF en coordinación con algunos de los otros grupos de trabajo para la implementación. Una de las recomendaciones fue la recomendación 17, que dice que la ICANN tiene que ser sensible al hecho de que los medios sociales están bloqueados en ciertos países, y en conjunto con organismos técnicos promueven alternativas creíbles.

Así que hemos mirado los servicios de chat de grupo tales como Slack y HipChat. Pero también empezamos a ver dos que se podrían utilizar para eludir quizá sitios web bloqueados.

Ha habido alguna discusión dentro del grupo en cuanto a si debemos considerar utilizar estas herramientas, y decidimos que necesitamos de hecho tener alguna conferencia telefónica para entender realmente algunas ideas acerca de estas herramientas. Y una de las herramientas más populares es el proyecto Tor. Aquí es donde tenemos nuestro orador invitado, David Goulet, quien es una persona involucrada en el proyecto Tor. Él accedió muy amablemente a participar en esta llamada el día de hoy. Así que me gustaría ahora cederle la palabra a David para que nos dé su presentación. David, tiene usted la palabra.

DAVID GOULET: Hola. Soy David. Soy de Montreal, así que estoy franco-canadiense, así que lo siento por mi acento o lo que sea. Es posible que tengan algún problema para escucharme o entenderme, pero voy a tratar de ser lo más conciso que pueda. Supongo que ustedes tienen todas las diapositivas. No puedo controlarlas, así que voy a pedirle a alguien al teléfono. Voy a decir siguiente diapositiva.

En primer lugar, muchas gracias a Glenn por invitarme. Lo conocí en Montreal y él tuvo la amabilidad de invitarme para que hable sobre el proyecto Tor.

Vamos a comenzar con la primera diapositiva que es la introducción. Yo he trabajado en el proyecto Tor durante casi un año. He sido voluntario durante tres años antes de mi actual trabajo. Con todo, he estado cuatro años con el proyecto Tor. Tenemos una misión global. Lo pueden leer ahí. No lo voy a leer de nuevo, pero la mayor parte es la tecnología, la defensa de la privacidad. Hacemos un montón de investigación. Tenemos por lo menos tres universidades de todo el mundo que

conozco que hacen investigación activa en la red Tor, con la red Tor. Y tenemos difusión múltiple en términos de libertad de expresión, censura, elusión y esas cosas.

Si va a la siguiente diapositiva ahora, ¿qué es Tor? El proyecto Tor creó hace un tiempo fue creado por el NRL que es el Laboratorio de Investigación Naval de los EE.UU... Este señor, [inaudible], y otra persona - no recuerdo exactamente.

DEV ANAND TEELUCKSINGH: Parece que alguien tiene... David, continuemos. Vamos a ver si el audio [inaudible] y lo solucionan.

DAVID GOULET: Básicamente fue creado para tener una forma de añadir una manera de comunicarse a través de Internet en anonimato de modo que se pueda preservar la privacidad de cualquier persona que la utilice. Por supuesto que había ideas militares detrás de eso y ahora se ha movido un poco hacia un proyecto después de unos años. No sé los detalles, pero ahora Tor es un software que se utiliza para el anonimato en línea. Es de código abierto completo. Todo lo que hacemos es de código abierto. No tenemos nada que vende o lo que sea. Todo nuestro trabajo es transparente en Internet lo que significa que las listas de correo son [inaudible]. Tenemos propuestas abiertas y esas cosas.

Para que la comunidad ha crecido bastante en términos de investigadores, desarrolladores, usuarios, y por supuesto [relé] operadores. Voy a entrar en lo que es un [relé] operadores.

Hoy en día, nuestra financiación en su mayoría proviene del gobierno basado en los Estados Unidos - así que el Departamento de Defensa, el Departamento de Justicia - Dependiendo del año tenemos becas o lo que sea. En este momento no tengo los detalles de nuevo, pero la mayor parte de nuestro dinero viene del gobierno estadounidense. También tenemos fundaciones y otras cosas.

Trabajamos hacia [inaudible] fuente de financiación. Así que si van a la siguiente diapositiva, que es básicamente [inaudible] para las personas en los EE.UU. Es un 501 (c) (3), que es para que las personas en los EE.UU. - o incluso los EE.UU., por si no lo saben - es una organización sin fines de lucro. En los EE.UU., tenemos una oficina en Cambridge y nuestro objetivo es, una vez más, la investigación y el desarrollo en el campo del anonimato.

Veámoslo. Si vamos a la siguiente diapositiva - la diapositiva cuatro - tenemos esta bonita estadística aquí y que la última vez que la revisé estimaba 2.1 millones de usuarios diarios de Tor. Eso significa que en la red tenemos esa cantidad de usuarios en cualquier momento.

Si vamos a la siguiente diapositiva, hay una gráfica - la diapositiva cinco - que conecta directamente a los usuarios. Esto es sólo 2015. Pueden ver que es más o menos estable en 2.1, tal vez 2.2, millones de usuarios.

Por cierto, voy a usar bastantes gráficas en esta presentación y aparece la dirección en la parte inferior de cada gráfica, me parece que es metrics.torproject.org. Todas las gráficas son accesibles. Puede cambiar las fechas, descargar un PDF, y así sucesivamente y así sucesivamente.

Voy a entrar en el modelo [amenaza] de Tor en la siguiente diapositiva. Antes de empezar, habrá partes técnicas y también iré a algunas partes menos técnicas. Creo que tenemos [inaudible], pero Tor es un proyecto descomunal, por lo que el objetivo es realmente para que ustedes entiendan todo el asunto en términos de tecnología, pero también en términos de comunidad y la importancia de los usuarios, ya que llega a las afueras de la parte de la tecnología que es la parte humana.

Voy a comenzar con esta diapositiva que es el modelo [amenaza]. Hace un tiempo - Tor tiene alrededor de diez años de edad. Tuvimos esta idea de lo que un atacante puede hacer cuando se tiene esta red. En esta diapositiva, imaginen que la red anónima podría ser Internet [inaudible] y Alice y Bob se conectan al Internet. Así que hay varios puntos en los que un atacante puede espiar, escuchar o ya sea ver o atacar a uno o a los dos participantes.

Ahora pasemos a la otra diapositiva, que es la siete. Hay una cosa muy importante - un aspecto importante - es necesario comprenderlo con la red Tor. Es el anonimato, no hay seguridad. Con esto quiero decir que proporcionamos anonimato en la capa de transporte, pero el problema es que la capa de aplicación siempre tendrá una [fuga] cuando se entra a la red Tor o cuando se sale de la red Tor. Afortunadamente, no sólo reparamos cuando se entra, sino que también reparamos la fuga de contenido -, pero al salir, ese es otro problema.

En este caso, en esa diapositiva, vemos que el anonimato está encriptado. He aquí: "Hola, Bob" "Hola, Alice" bla, bla, bla. Son puras sandeces. Todavía no es anonimato debido a que, tal como lo conocemos ahora, gracias a nuestro amigo Snowden es que una gran

cantidad de datos en Internet están siendo vigilados - [inaudible] básicamente basado en meta datos. El anonimato se vuelve muy importante aquí.

Si nos vamos a la siguiente diapositiva - diapositiva ocho - la cosa es que no es sólo una ilusión, en términos de tecnología, sino también hacia la ley. Si tenemos agencias gubernamentales o corporaciones o gobiernos, hay declaraciones que dicen: "Prometo que no voy a mirar. Prometo que no espiamos a nuestros ciudadanos. No vamos a leer su correo electrónico", o lo que sea. Todo esto no es suficiente por desgracia hoy en día. Tenemos un montón de frases en esta diapositiva que sólo dicen que no es posible tener el anonimato con sólo decir que se pueda demostrar que era yo.

Esta siguiente diapositiva - diapositiva número nueve - tenemos diferentes intereses de los diferentes grupos de usuarios. Este anonimato no sólo puede aplicarse al gobierno, por ejemplo, donde en la primera base con Tor y diez años atrás, así era. El objetivo era proporcionar el anonimato para cualquiera de los agentes en el campo o militar o sólo para funcionarios del gobierno en empresas extranjeras.

Pero el juego ha cambiado bastante. En Tor, hoy en día, contamos con activistas de derechos humanos, empresas, particulares, por supuesto, gobiernos. Se amplió a - se puede ver [inaudible] ahí. Los ciudadanos privados serían los ciudadanos normales. Cualquiera en el campo. Sabemos que agentes no sólo de los EE.UU., pero de otros gobiernos lo utilizan en todas partes del mundo. Necesita de todos esos cuatro aspectos diferentes, que son [inaudible], seguridad de red, por supuesto, privacidad. Ese es el viejo concepto. Y el tráfico [inaudible] es

también un buen [inaudible]. Y tenemos esos porque hay enemigos - adversarios, diría yo - que tratan de exponer a Tor fuera del anonimato. Es toda una carrera.

Si nos vamos a la siguiente diapositiva - la número 10 ahora. Este es el diseño [más simple] que puedan ver. Me voy a mover hacia [inaudible] explicar por qué se llegó a esto.

Tenemos a Alice y a Bob en el Gmail y retransmiten. Por supuesto, esto es un problema porque si vamos a la siguiente diapositiva - la número 11 - resulta que [inaudible], bueno, entonces, intercepta los ataques o lo que sea. La censura, también. [Inaudible] punto único de fracaso.

Afortunadamente, la Internet como la conocemos ahora, sí, se trata de una web. Es redundante. Vamos a través de diferentes caminos, dependiendo de las fallas o no. Pero todavía usamos Gmail en nuestra vida diaria, que es [inaudible].

Bueno, esa es la [regla] de la aplicación. Entiendo, pero aún así, contamos con la misma red y así sucesivamente y así sucesivamente que es controlada por entidades individuales. Así que eso es un problema - el anonimato, me refiero.

Así que ahora pasemos a la diapositiva 12. Entonces tenemos esta idea. De acuerdo, vamos a añadir varios relés para que ni una sola pueda [inaudible] Alicia en este caso. Cuanto más diversificamos su camino hacia su destino, tenemos una suposición razonable de que es más difícil de atacar a Alice, escuchar a Alice, o hacer cualquier posible ataque. La censura también [inaudible].

La red Tor - Tor significa The Onion Router, el enrutador cebolla. Hay una razón por la qué es una cebolla. Vamos a ver que en la siguiente diapositiva - diapositivas 13 - lo que ocurre es que cada relé... Alice se comunicará a través de cada relé y luego [inaudible] Bob. Así R1 aquí, en este caso aquí sería el nodo de entrada, entonces el R2 será nodo intermedio y, a continuación, R3, que es un nodo de salida. Y existe [M3] y en medio de la red Tor existen propiedades muy diferentes. Se comportan... Bueno, esperamos que se comportan como los demás, al igual que cualquier otro nodo, pero todavía tienen diferentes roles.

En este caso, lo que va a suceder es que Alice va a crear un camino para Bob, por ejemplo: "Bien, voy a escoger a R1, R2 y R3 y conozco esos relés de un documento conocido", lo que nosotros llamamos el consenso. El consenso está creado por nueve autoridades de directorio en la red Tor. Por desgracia, no tengo una diapositiva para eso. Pero tenemos ahora nueve servidores alrededor del mundo que están a cargo de personas de confianza y esos servidores son responsables de medir - no medir, pero sólo la creación de lo que llamamos el consenso que es un documento que todos están de acuerdo en y que contiene todos los relés de la red Tor que se pueden utilizar. Este documento básicamente detalla cada relé con sus claves de huellas digitales [inaudible]. Eso significa la importación de la IP. Y algunos otros datos útiles.

En ese caso, cuando Alice se pone en marcha, el primer movimiento que hace es llegar a este consenso, porque este consenso es la vista de la red. Si Alice ya tiene todo un consenso, intentará llevarlo a través de un directorio de caché, que básicamente es cualquier relé en la red Tor, dependiendo de algunos requerimientos, pero sobre todo, todos los

relés. O bien, si Alice no tiene un consenso, dicho documento, lo va a buscar en esos nueve directorios. Y la forma en que lo sabe es porque esas autoridades de directorio están codificadas en el código de Tor.

Así que las claves son públicas y también sus direcciones y algunas otras cosas útiles. Es completamente [codificado-R]. Así que eso significa que cada cliente, cada relé de Tor, todo lo que usa Tor sabe dónde obtener los directorios [inaudible].

Así que ahora regresamos a nuestra diapositiva, Alice ha [puesto en cero] red. Entonces ella puede elegir R1, R2, y R3. Así que con eso en mente, en el consenso, cada relé tiene una clave. Se asigna una clave pública en el consenso. Así que ella sabe que puede cifrar una conexión a R1 y R3.

Si miran esa diapositiva, las capas son claras. Verde, amarillo y azul. La primera capa es R1. R1 es la clave verde. Cuando Alice encripta, ella va a tener esta línea blanca que es el contenido, y luego se va a hacer tres capas para cada [inaudible]. A continuación, envía [inaudible] de nuevo a R1. R1 elimina la capa, sabe dónde enviarlo después; la información de los paquetes. Luego lo envía a R2. R2 elimina la capa, la capa amarilla. Y entonces R3 eliminará la última capa.

Así que lo que pasa aquí es que R3 es un nodo de salida y R3 tiene acceso a los contenidos que se cifraron en un principio. Ven la línea blanca. Esto es importante.

Volvemos al anonimato frente a la seguridad. Como un [servidor global] o como cualquiera - un atacante que puede ser R1, R2, R3 o, no se sabe de donde viene. No se sabe lo que está en los datos, en el centro. Pero

la salida lo sabe. Así que la salida sabe a dónde va y cual es el contenido, pero no se sabe de parte de quién viene.

Así que tenemos esta cosa en Tor en la que realmente se necesita utilizar seguridad también en términos de encriptación. SSL, OTR, PGP o lo que se necesite, para que la salida no pueda husmear sus datos.

Si vamos a la siguiente diapositiva, la diapositiva 14, es una capa de cebolla agradable [de las capas de cebolla]. Así que en cada relé pelamos una capa.

Voy a dejar tiempo para preguntas, así que no dude en preguntar. A veces puede ser complicado. Bueno, vamos a ir a la siguiente diapositiva, la diapositiva 15.

Este es el número de relés que tenemos en la red Tor hasta ahora. Lo tomé ayer en la noche. Eso significa que... Creo que tenemos alrededor de 6,800 relés. Eso es 6,800... Bueno, eso significa que la gente pone en marcha esos relés - cualquiera. Así que a un relé lo puede manejar cualquier persona que así lo deseé. Tenemos voluntarios en todo el mundo.

Si deciden visitarlo, tomen nota, porque es una increíble visualización de la red Tor. Si pueden visiten torflow.uncharted.software. Si van allí, es una increíble visualización de toda nuestra red en todo el mundo.

Y los puentes. Los puentes, disponemos de 3,000. No hablé de ellos. Los puentes son relés que no se anuncian en el consenso. La razón es que cuando la censura opera en un país u organización o lo que sea, uno de los [inaudible] red Tor - Tenía una diapositiva de eso - es bloquear toda

la IP [retransmitida] porque aquellas son conocidas, [porque] se puede conseguir este consenso.

Ahora, los puentes no están en el consenso, pero hay diferentes maneras de conseguirlos. No estoy seguro si tengo una diapositiva sobre eso, pero se me ocurre, por ejemplo, que hay una manera de enviar un correo electrónico a una dirección de correo electrónico específica y se pueden recibir puentes por correo electrónico. Luego se toman estos puentes y se ponen en la configuración de Tor y ese será el punto de entrada a la red Tor. Dado que no es conocido por nadie, nisiquiera por el consenso, se puede evadir la censura. Voy a regresar al tema de los puentes con atacantes activos.

Si vamos a la siguiente diapositiva, este es el ancho de banda total del relé, en la diapositiva 16. Se puede ver en este momento que nuestro ancho de banda anunciado, lo que significa que en cada ancho de banda relé anunciado, tenemos autoridades de ancho de banda que miden en todo momento los relés y tratan de hacer una estimación para poder seleccionar una ruta mucho más inteligente. En este caso, somos alrededor de 140 gigabits por segundo de ancho de banda posible. Y esta [historia] ancho de banda es lo que creemos que se utiliza. Una vez más, esto es una estimación. Esto no es tan preciso, pero nos da una idea de lo que ocurre.

Si nos vamos a la siguiente diapositiva - ahora la número 17. [Las carreras armamentistas], son un gran problema para nosotros. Tenemos un poco de [inaudible] en Internet por múltiples razones - sistema de vigilancia, censura. Se pueden imaginar lo que cualquier país o régimen actual pueden hacer cuando [hackean] su Internet.

Si nos vamos a la siguiente diapositiva - la 18. Hablé un poco justo antes de la forma de bloquear las redes Tor. Hay múltiples maneras. En primer lugar, por supuesto, está bloquear el [inaudible]. Hay nueve de ellos. Son conocidos. Y si se bloquean todos, bueno, nadie puede iniciar el protocolo bootP porque no pueden conseguir ese consenso, ese documento que explica y detalla la [visión] de la red.

Se ha hecho en los países, en varios países, pero hay una manera de esquivarlo. Es por esto que existe [inaudible] caché, que cada relé puede almacenar el consenso en caché. Pero por supuesto que se necesita iniciar el protocolo bootP en algún momento, pero se puede llegar a un consenso de salida, desde otra persona, y luego empezar a dar inicio con el protocolo bootP y esas cosas. Así que esto no es como una forma ideal. También se pueden bloquear todos los IP de los relés, como ya he dicho.

El filtrado de [bahías] en la huella digital de la red de Tor. Así Tor, cuando se conecta desde el relé para retransmitir, utiliza TLS. Y dentro de ese período de sesiones TLS hay lo que llamamos la piel de cebolla o las capas de cebolla. Así que hay un poco de cifrado, pero esto TLS, tratamos de se que vea tanto como nos sea posible a [HTTPS], pero no es tan fácil todo el tiempo. Así que cualquier otra cosa previene a los usuarios de encontrar el software de Tor.

Tengo un par de diapositivas que enseñarles, una captura de pantalla de páginas en torprojcect.org que secuestran en diferentes países para mostrar cómo evitar que los usuarios [de hacerlo].

Si nos vamos a la siguiente diapositiva - diapositivas 19 - este es un ejemplo de conexión directamente con los usuarios de Egipto. Si se

acuerdan de Egipto, se puede ver que esta línea baja. Eso fue cuando, durante tres días, si mal no recuerdo, cerraron por completo la Internet. Se puede ver que la caída fue muy importante y esos puntos muestran censura [eventos]. Bueno, e basa en la estimación. Pueden obtener algo más de información [inaudible] torproject.org [que lo explica].

Pero esto es algo interesante donde podemos ver cómo los países realmente tratan de censurar o cuando de hecho existe un movimiento en Internet o cosas que ocurren en su momento.

Les voy a mostrar la siguiente diapositiva, la diapositiva 20, se trata de Libia. Cuando esta guerra hacía estragos en Libia hace cuatro años o algo así, se puede ver esta enorme caída en que fueron descartados por completo. Creo que incluso les cerraron la Internet por unos momentos. Luego empieza a crecer.

Pero la enorme línea que sube a casi 300 usuarios, por lo general es cuando se tiene actividades políticas muy importantes en el país. Tengo varios diagramas. Acabo de tomar algunos. Pero desde el Congo, de Ucrania, de - tenía otro. No recuerdo el país. Dónde se puede ver [inaudible]. Se puedes ver todos los eventos de censura o eventos políticos con [un aumento de usuarios de Tor].

Si vamos a la siguiente diapositiva - diapositiva 21 - se trata de Irán. Así que Irán ha sido uno de los países más activos en bloquear a Tor. Lo hicieron en múltiples formas. Pero de alguna manera, en enero de 2011 se dieron cuenta de un poco de las cosas y desistieron. Así que casi cero [clientes]. Y si no me equivoco - Puedo estar equivocado aquí - bloquearon Tor basándose en [TPI] de Internet y encontraron un modo de identificar la conexión [TLF]. Luego, según lo recuerdo, Tor acababa

de cambiar uno de los elementos [TLF] así que retrocedimos y entramos por el firewall iraní. Se pueden ver un poco con [inaudible] todas nuestras métricas. Muy impresionante.

Ahora, el último diagrama que tengo para esta ronda es la diapositiva 22 donde aparece China. China es todo un adversario. Son bastante impresionantes. Bloquearon a Tor de múltiples formas. Bloquearon a Tor ... Las cuatro formas de bloquear a Tor, bueno, ellos hicieron todas. Y también una de las cosas que hicieron fue enumerar puentes. Creo que hay tres o cuatro maneras diferentes, se puede obtener un puente, ya sea por correo electrónico - se va al puente torproject.org y entonces se puede conseguir un puente desde allí. Así que hay múltiples maneras. Ellos [inaudible] todos ellos y los bloquearon. No sólo eso, pero ahora sabemos que cuando hay una conexión de salida [TLS] que parezca sospechosa o lo que sea, de hecho se reconectan a la misma para intentar sacar como una huella digital. Esta es una de las formas en las que de hecho son muy eficaces en el bloqueo de Tor. Estos diagramas muestran que a mediados del año 2010 de hecho tuvieron bastante éxito. Este es un diagrama viejo, pero creo que hasta el 2015 es más o menos lo mismo.

La siguiente diapositiva, diapositiva 23. Las siguientes dos diapositivas esencialmente son las páginas que recibe la gente en diferentes países sobre lo que es torproject.org. Una forma de reforzar o censurar o detener a torproject.org sería simplemente no permitir la descarga del software.

En la primera de ellas aparecen los Emiratos Árabes Unidos, Bahrein. Se ven amigable. Es un buen payaso. O no un payaso, pero me refiero a

una señora que dice lo que es malo para navegar de forma segura. Esta cosa del proyecto Tor no es buena, ¿no?

Si vamos a la siguiente diapositiva - diapositiva 24 - aparecen unos simpáticos personajes que dicen que es un problema y así sucesivamente y así sucesivamente. Así que la gente, cuando va al proyecto Tor y ven eso, no piensan que sea censura. Piensan que sólo es ser para su propio bien. Eso es un poco del problema aquí.

Si ahora vamos a la diapositiva 25, ¿a quién nos enfrentamos? Ya les hablé un poco sobre China. Existen fire-walls del gobierno. [Inaudible] frente a Irán frente a China. Sabemos que un montón de países están tratando de bloquearlo o [inaudible] de moverlo lejos. Incluso las empresas estadounidenses han dedicado software para bloquearlo.

Una de las cosas [inaudible] es también [inaudible] proporciona una [opción] para sus usuarios sólo para bloquear a Tor, y por supuesto, creo que sólo bloquean a Tor al bloquear las IPs o conseguir la firma de TLS. Pero aún así es algo que ahora se está poniendo en el producto cada vez más comercial para bloquear a los usuarios de Tor.

Si vamos a la siguiente diapositiva, otra vez, Irán 2015. Se puede ver que lo bloquearon bastante de nuevo. Cada vez que hay una respuesta a cualquiera de las actividades políticas o acaban de comprar un nuevo hardware, o en algún momento sus investigadores encontraron una manera de simplemente filtrarlo por completo.

Esta carrera armamentista que enfrentamos es una carrera constante en este momento. Vemos esos eventos de censura que ocurren en

todos los países de todo el mundo todo el tiempo. Un puñado de países [inaudible], pero hay más [inaudible].

Si vamos a la diapositiva 27, como una red de anonimato, la seguridad de Tor proviene de la diversidad de los usuarios. Si está en ... digamos que está en un país, un país [inaudible], y es el único que utiliza Tor. Bueno, digamos que va a llamar muchísimo la atención. Es muy fácil ver el tráfico de Tor.

Así que el nombre del juego con Tor para el anonimato es la diversidad y el mayor número de usuarios que se pueda. Siempre y cuando haya actividad hay anonimato porque entonces se ve igual que como todos los demás.

El punto número dos es que hay 50,000 usuarios en Irán, lo que significa que casi todos son ciudadanos normales de alguna manera porque todos generan un tráfico normal. Y tantos más usuarios como sea posible, bueno, hay mejores posibilidades de anonimato porque de hecho es fácil encontrarlos cuando hay pocos usuarios.

Está la historia de un estudiante en [inaudible] quien de hecho utilizó la red Tor para enviar un correo electrónico a - no recuerdo si estaba chantajeando o lo que sea. Pero él era el único en el [inaudible] de la red, por lo que fue muy fácil [agarrarlo]. Así que la diversidad y una gran cantidad de usuarios es realmente muy, muy importante para el anonimato.

Diapositiva 28. Esta es una pieza del rompecabezas. Hemos visto que el último equipo de [hacking] y las fugas [inaudible], y son noticia, si algunos lo recuerdan, donde venden software espía (spyware) para

empresas, el gobierno, o lo que sea y uno de esos de hecho husmeaba activamente a los usuarios de Tor . Así que suponemos que se trata de una pieza del rompecabezas, pero no es una solución plena a prueba de balas porque si se tiene hardware o software al que se le puede atacar - spyware. ¿Realmente se tiene una copia original de Tor?

En la parte técnica, [inaudible] recientemente - quiero decir recientemente... creo que ha sido un año, tal vez menos. Tor es... Hemos creado esta cosa que se llama [estructura productiva]. Tor se construye en distintas máquinas por diferentes personas y todos ellos coinciden con el mismo [inaudible] al final. Eso significa que es la misma copia en todas partes, lo que llamamos la [estructura productiva].

Existe una gran persona en Tor que trabaja en eso y ha creado el [productive-build.org] o algo así, y ahora [inaudible] ha casi el 80-85%, si no el 100% actual de sus paquetes que son de [estructura productiva].

Se trata de un enorme esfuerzo de Tor, así que cuando le ofrecemos el binario Tor a la gente de todo el mundo, sabemos que es la copia exacta que pensamos que debe ser.

Si vamos a la diapositiva 29, se trata de una diapositiva del documento secreto de la NSA que fue dirigido por Snowden. Una de las cosas con Tor es que no les gusta en absoluto. Eso fue en el 2012, osea hace tres años. Así que eso es [inaudible]. Pero sí, huele mal y no les gusta mucho.

Si vamos a la diapositiva 30, creo que de hecho ese logo estaba en una de las diapositivas y con esa cita todavía en busca [inaudible]. Dijeron que [inaudible]. No lo creemos. Existen otras varias [rondas] en la red que utilizan diferentes cosas como [inaudible] o algunas de las

alternativas. Tienen diferentes modelos de negocio. También tienen diferentes maneras de conseguir el anonimato de Internet. Pero en general, Tor fue el que la NSA estudió bastante. Sabemos de [esto] a causa de esas diapositivas. Sabemos que tiene algo de tracción.

No sé si sabían sobre eso, pero hace dos o tres días empezó esta historia de que el FBI de hecho financió una universidad - una universidad [inaudible] - para [inaudible] usuarios de Tor, que fijamos en julio, el pasado julio. No el pasado julio, pero julio del año pasado. Esa investigación para el anonimato de los usuarios de Tor que de hecho sucedió y le proporcionó al FBI con IPs para que los pudieran condenar.

Así que sabemos a ciencia cierta que gente mala utiliza Tor. Eso lo sabemos. Pero creemos que no es el caso de uso principal. Tengo un gráfico para demostrarlo.

La diapositiva 31 muestra esa percepción. ¿Qué es Tor? Luchamos bastante en las noticias acerca de que en el [inaudible] Tor. Por lo general, cuando alguien escucha un poco acerca de Tor es porque se enteró de la web oscura o la web profunda. Tratamos de no utilizar esa frase porque, para nosotros, Tor es sólo Internet de una manera que se accede de forma distinta, pero de manera que protege su privacidad.

Así que es una gran percepción de un problema de cara al público y también hacia el gobierno o agencias que en realidad ven a la red de Tor como algo malo o que no es bueno.

Si vamos a la diapositiva 32, hay varias maneras de [inaudible] Tor en formas legales. ISP [inaudible], por ejemplo. Ejecutar un relé de salida es muy difícil para los ISP, porque obtienen una gran cantidad de avisos o

quejas [inaudible] porque el tráfico no es todo el tiempo lo bastante [claro]. Así que eso hace que el ISP nos odie más y más y más. Eso es desafortunado. Todavía batallamos pero lo solucionamos la mayor parte del tiempo. Ahora tenemos casi 7,000 relés.

[Inaudible]. Eso es fácil. Recientemente - y creo que aún así, es todavía un proceso en curso para la gente en los EE.UU... No se puede ir a healthcare.gov a través de Tor. Eso es lamentable porque proteger en Internet su estado de salud o sus condiciones de salud o simplemente tratar de obtener un seguro es algo que debemos proporcionar privacidad [inaudible] y hasta el momento no hay ninguna.

La siguiente diapositiva, diapositiva 33. Todos recuerdan a esa persona de [Prominola], a Snowden. Debido a esto [inaudible] aquí en la parte superior derecha, y él también defiende bastante a Tor. Tenemos un poco de afluencia de usuarios en algún momento y también intereses de múltiples maneras, porque esta historia recorrió el mundo.

Si nos vamos a la siguiente diapositiva, en la diapositiva 34, esto es un trabajo enorme en la conexión [inaudible] de usuarios. La cosa es que esto está también [muy] vinculado a una botnet que estaba activa en Tor y que cuadruplicó nuestros usuarios. Teníamos más que eso - 5 millones de usuarios. Así que eso es con una botnet, pero también hubo un enorme [efecto] Snowden, después de un tiempo la gente decía: "Oh, ¿qué es esta cosa Tor? ¿Por qué lo utiliza esta persona?" Despertó interés.

Así que para decir que esta línea regresó cuando cancelamos la botnet, pero todavía son 2 millones de usuarios, no 1 millón, por lo que el efecto de Snowden fue muy fuerte.

Si vamos a la diapositiva 35, creo que nada más la puse ahí porque ya no me acuerdo. Se suponía que iba antes. Pero sí, la [inaudible] que conecta a los usuarios de Turquía, y justo antes de septiembre, fue el - no lo recuerdo. Me chocan mis notas, pero creo que esta diapositiva es [inaudible], así que vamos a ir a la siguiente, diapositiva 36.

Estoy llegando al final de mi charla. Yo sólo voy a hablar un poco acerca de los servicios ocultos. Así que los servicios ocultos es algo que puede ser que todos hemos escuchado y que de hecho aparece en las noticias directamente conectado a la web oscura, y son esas direcciones de cebolla [de .onion].

Así que esto no es la [clásica] búsqueda de DNS. Un .onion es una dirección en la que se puede llegar a [un servicio] en Tor. Lo bueno de servicio [inaudible] es que los clientes entran en las redes y nunca salen de ahí. Se llega a un servicio que está dentro de la red Tor por lo que no se pasa por una salida mientras sus datos salen [sin criptar] en la Internet abierta.

Me voy a quedar en la diapositiva 36. Tenemos [inaudible] y Facebook - Recientemente Facebook creó su propia dirección de cebolla. Esto es muy bueno porque hace una distinción entre la Internet abierta y la web oscura, o lo que nos gusta llamar el espacio cebolla. Visitar [inaudible] es casi lo mismo porque se llega a Facebook a través de un .onion o .com. Para nosotros, visitar a un .onion, es sólo una forma de llegar a un servicio de una manera segura, pero no debe ser visto como diferente de la Internet abierta. Sí, tiene diferentes mecanismos, pero todos tenemos diferentes mecanismos para un montón de cosas en torno a Internet de todos modos. Así que Facebook [inaudible].

Intentamos defender otros servicios que proporcionan direcciones de cebolla, ya que permiten que los usuarios lleguen a Facebook o [inaudible] utilizando el anonimato, pero también de una manera muy segura. Voy a explicar por qué esos servicios son mucho más interesantes.

Si nos vamos a la siguiente diapositiva - la diapositiva 37. Hay una dirección en la parte inferior porque hay seis o siete imágenes para los servicios ocultos. Para explicárselos de una vez por todas, acabo de poner un gráfico, pero muestra todo el asunto. Tienen esta dirección en la parte inferior y pueden leer sobre eso y todo. Pero yo sólo voy a hacer esta introducción aproximada de lo que es [inaudible] servicio o servicio cebolla.

Alice quiere conectar con Bob. Digamos que Bob tiene un servicio web. Digamos que es Facebook. Quiere ofrecer un servicio a través del espacio de cebolla. Ahora, el servicio de Bob se va a conectar con tres puntos de introducción - la IP1, IP2, IP3 y que se ven en esta imagen. Esos puntos de introducción son sólo un circuito a través de Tor. Así que de tres [inaudible] circuitos como vimos antes en la presentación. Y Bob va a mantener este circuito abierto a las IPs.

Ahora, Alice va a - [inaudible] va a conectarse a Bob con esta dirección de cebolla, y será capaz de hacerlo con esta dirección de cebolla. Es una [ceniza] básicamente de la clave pública de la [inaudible] y alguna otra información. La razón es que esta dirección larga le da un lugar para ir en [DHT] que es lo que llamamos un directorio de servicio oculto, que son básicamente los relés que se ajustan al perfil que es el tiempo de

funcionamiento de más de 96 horas, de forma rápida y ancho de banda, con algunos requisitos así.

Este saluda a [DHT], o un anillo y con la huella digital del [inaudible], del relé que tiene el directorio de servicio oculto. Así que Alice va a conectarse a [inaudible] porque con la dirección de la cebolla que ella sabe que [inaudible] para conectarse. Ella va a descargar lo que llamamos un [agente] descriptor de servicio que es un documento que explica dónde ponerse en contacto con Bob.

En este documento, se encuentran las IP, el punto de introducción a las direcciones 1, 2, y 3. Así que Alice se conecta al punto de introducción, una de [inaudible] punto de introducción. Y en ese punto hay un circuito desde Bob que es [inaudible] y Alice los va a [llamar]. Así que Alice le va a decir a Bob, "Por favor, únanse a mí en este punto de encuentro."

Así que Alice se conecta a IP1, a continuación, puede hablar con Bob a través del circuito. Entonces Bob se conecta de nuevo al punto de encuentro. Y Alice se conecta al punto de encuentro y ambos se conectan y ahora tenemos toda esta conexión entre Alice y Bob. Eso es todo a través de la red. Eso nunca existe en la red. Tienen algunas propiedades agradables de secreto y de hecho ningún contenido se filtra de entrada o de salida en la red Tor.

Así que esto es más o menos los servicios ocultos. Por favor, siéntase libre de hacer preguntas porque la mayor parte de mi trabajo en este momento en Tor es en los servicios ocultos. Si vamos a la diapositiva 38, ya casi termino. Esto es a partir de septiembre. De hecho no, esperen- mucho antes de eso. Pero esto es sólo de septiembre a noviembre. Hay estadísticas de los servicios ocultos. Tenemos dos estadísticas diferentes

que se recogen en [privado] de maneras anónimas que nos dice la cantidad de tráfico en la red Tor.

En estos momentos cerca de 900 megabits por segundo del tráfico en toda la red Tor son de servicios ocultos. Esto es alrededor... me parece que nuestra estimación es de alrededor de 5.6% de todo el tráfico de la red Tor. Así que esta es la razón... Esta es una de las buenas razones que usamos este gráfico cuando hicimos este trabajo para que podamos demostrar que realmente Tor no es del todo mal tráfico que pasa a través de los servicios ocultos de mercado para las armas o cosas completamente malas en términos de tráfico humano y así sucesivamente y así sucesivamente. En realidad no es cierto. No sabemos cuál es el porcentaje de ese tráfico, pero aún así es un porcentaje muy pequeño de toda la red Tor.

Si vamos a la diapositiva 39, esta es la cantidad de direcciones únicas de cebolla que vemos en todo momento en la red Tor. Alrededor de 30, 000 [en todo momento] que están vivas. Tenga en cuenta que las direcciones de cebolla las utilizan los servicios como un servidor HTTP, un servidor de correo, pero también hay un montón de aplicaciones. Una de ellas se llama [Rickoshare]. Podemos ir a [rickoshare.im], que es una aplicación de chat que utiliza los servicios ocultos y dos personas - dos servicios ocultos - y pueden charlar en Tor. Eso crea mucha más direcciones de cebolla. Pero en [todo momento], 30,000. Esa es nuestra estimación.

Entonces si vamos a la diapositiva 40, se trata de una captura de pantalla del navegador Tor. Así es como la mayoría de las personas realmente utilizan Tor. Así que si va a torproject.org, puede descargar

este paquete navegador Tor. Es, básicamente, un Firefox mejorado con capacidades Tor y también varias privacidades [inaudibles].

Tenemos un gran equipo Tor que trabaja en eso, un gran equipo que trabaja en eso. Son gente increíble y hacen un trabajo increíble. Esta es una maravillosa pieza de trabajo que es [la estructura productiva].

Finalmente, la diapositiva 41. Esto es [inaudible] en el móvil, Androide. No estoy seguro de si finalmente tienen iOS ahora mismo, pero [inaudible] comprobarlo. Pero por lo menos [inaudible] muy agradable. Puede usar Tor en su teléfono móvil. Esto ha ganado terreno últimamente. Tuvimos algunas personas de Mozilla en el equipo de Firefox OS que trabajan con nosotros para operar en el móvil. Tor también tiene un modo particular de Firefox que sería bastante impresionante en términos de usuarios y alcance. Pero básicamente así es como funciona.

Voy a parar aquí, si ven la diapositiva 42. Por supuesto, muchísimas gracias. Hablé 41 minutos, así que eso significa que tienen 20 minutos, chicos, o más que eso. No me importa que hagan tantas preguntas como deseen, siempre y cuando pueda contestarlas. Gracias.

DEV ANAND TEELUCKSINGH: Gracias, David. Gracias por esa presentación tan informativa. Hay un buen número de preguntas que los participantes harán. Primero tengo a Glenn. Así que Glenn, por favor, tiene la palabra.

GLENN MCKNIGHT: Gracias. Una vez más, David, muchas gracias por su presentación. Me gustaría leer un par de preguntas del chat. Me gustaría volver. Tuvimos una pregunta de Alfredo Calderón de Puerto Rico. Él es de ISOC de Puerto Rico. Su pregunta era con respecto a - sólo estoy retrocediendo.

Fue con respecto a [dot.dot.go] anteriormente. Él pregunta: "¿Es verdad que se anuncia como buena para escuelas y grupos privados?"

DAVID GOULET: Así que [dot.dot.go] como un servicio, lo anunciamos como una solución para Google hacia la mejora de la privacidad. Debido a que no mantienen registros, también las solicitudes de búsqueda. Así que sí, lo es. Si entiendo bien la pregunta, sí, es una mejora desde Google. Esta es una de las razones por las que de hecho se agrega una dirección de cebolla muy temprano, para que la gente pueda llegar a ellos en una [forma] de - a través de la red de anonimato y privacidad. Así que espero que hay respondido a su pregunta.

GLENN MCKNIGHT: La segunda pregunta de la charla. Escuchen todos, David no está en Adobe Connect, así que me estoy tomando la libertad de leer las preguntas que se publican. La segunda pregunta es de Satish de India. Creo que es de [inaudible]. Le pregunta a usted, David. Él ha sido un gran fan y usuario de Tor desde hace ya varios años. Creo que es sumamente valioso, que salva vidas. Usted mencionó la semana pasada que la acción conjunta de SMU / SEI con la policía. Esto parece hacer que Tor aparezca vulnerable. ¿No sería un terreno peligroso?

DAVID GOULET: Es una pregunta muy interesante. En este momento, todo el trabajo en Tor es de código abierto. Es un mejor esfuerzo. Tenemos desarrolladores, investigadores. He estado haciendo esto durante muchos, muchos años. Pensamos que hacemos nuestro mejor trabajo. Creemos que nuestros usuarios son lo más importante. La seguridad de nuestros usuarios es muy, muy importante. Así que esta es la razón por la que todos nuestros procesos de desarrollo, los procesos de investigación, están siempre, siempre, siempre basados en la seguridad del usuario y la seguridad del usuario - y también para no romper ningún anonimato.

Ahora, siempre vamos a enfrentar las amenazas de los investigadores de todo el mundo, ya sea en agencias o universidades del gobierno estadounidense que realmente tratan de quebrantar a Tor porque eso vende un montón de periódicos. Pero también mejora la seguridad de Tor.

Así que yo diría que debemos seguir usando Tor. Eso es seguro. En nuestro trabajo, entre mayor financiación se consigue, mayor estabilidad se consigue en nuestra organización. Mejor podremos abordar esas cuestiones, y también podemos mejorar los servicios en este momento.

Sólo por dar un ejemplo, sé que tenemos [próxima generación] servicios ocultos, que con esta propuesta [de próxima generación] de servicios ocultos que se creó hace tres años, ese ataque que FBI y CMU nos hizo no podría ser posible porque estamos conscientes de las cuestiones que

existen. Todavía queremos arreglarlas, pero se necesita un poco de esfuerzo de ingeniería y también de la investigación.

Yo no diría que este es vulnerable porque en Tor estamos muy, muy activos en las últimas investigaciones, en respuesta a las amenazas y vulnerabilidades y derivamos la información al público con nuestro blog y lista de correo electrónico y un nuevo software.

Yo no diría que es vulnerable, pero tenga en cuenta que no es una bala de plata. Ese siempre es el caso de cualquier software.

DEV ANAND TEELUCKSINGH: Gracias, David. Gracias, Glenn, y gracias David. El siguiente orador es Lutz Donnehacke. Lutz, tiene usted la palabra. Adelante.

LUTZ DONNEHACKE: Gracias. Gracias por la maravillosa presentación. Regresando a la ICANN veo que una gran cantidad de servicios de la ICANN van a requerir de inicio de sesión y nombres reales al utilizar el servicio. Por ejemplo, la nueva plataforma de aprendizaje requiere que dé su nombre completo con el fin de ver de un simple vídeo de introducción.

La pregunta que tengo es ¿tenemos un buen argumento para decirle a la gente de la ICANN que paren de desanonimizar a los usuarios, que paren de descubrir quién está usando qué servicio? ¿Tenemos un muy buen argumento para el uso de la plataforma de aprendizaje sin saber quién está accediendo los archivos individuales? Gracias.

DAVID GOULET: Bien. Esa es una cuestión muy compleja. Hay un montón de razones por las que se inicia sesión con nombres reales o no. Tal vez son buenas, tal vez no lo son. Pero una de las cosas que tiene que tener en cuenta es más un servicio de registros de nombres reales, crea un rastro digital de lo que la persona ha estado haciendo o está haciendo. Se trata de metadatos que son muy útiles como una realidad hoy en día que estamos [inaudible] de vigilancia está en todas partes.

Ahora, si tiene los datos, eso significa que puede - si usted tiene esos datos, eso significa que lo puede regresar a las agencias si tienen una orden legal o cualquier cosa así. Pero también las leyes cambian en diferentes partes del mundo. No es algo que sea súper estable. Esto significa que si tiene la información en algún momento, podría no serle útil en otro punto. Se podría utilizar en contra de los usuarios o no.

Mi argumento aquí sería que si no hay una necesidad real de añadir los nombres que no sea justo para, no sé, estadísticas o una mejor entrega de publicación de anuncios, no deberíamos porque perdemos esta parte de la privacidad. Y también, estos datos, no sabemos para qué los van a utilizar en contra o para después de múltiples años o en el próximo mes. Una vez más, podría haber argumentos para tener nombres reales. Por ejemplo, si quiere hablar en el foro, por ejemplo. Quiero saber si realmente hablo con Glenn o no. Pero depende. Todavía voy a utilizar este argumento de datos [inaudible].

DEV ANAND TEELUCKSINGH: Gracias, David. Reviso a ver si hay alguna pregunta. Bueno, en realidad, tengo una pregunta, David. Antes tocó el tema. Mucho de esto parece haber sido dirigido a las computadoras de escritorio y así

sucesivamente. Pero ahora [inaudible] cada vez más se tiene acceso a Internet desde un dispositivo móvil. Bien. Por lo que se tiene un Androide como una plataforma compatible, pero, ¿se puede instalar Tor en, por ejemplo, a nivel de router de manera que todos los dispositivos que estén conectados al router puedan usar Tor?

DAVID GOULET: Así que la pregunta es ¿puedes tener dispositivos - puede que tenga, digamos, un router? ¿Para que entonces todos los dispositivos conectados al router, pueden entrar a través de Tor? ¿Esa es la pregunta?

DEV ANAND TEELUCKSINGH: Sí.

DAVID GOULET: Así que, sí, esto es totalmente posible. Hay varias maneras de hacerlo. Ahora, sólo para que lo tengan en cuenta, es la aplicación - Tor funciona en la capa de transporte. Así que, básicamente, lo hace en TCP para poder ser anónimo. El problema es que cada aplicación, como se diseñan hoy en día, derraman una enorme cantidad de información sobre usted.

Esto significa que si tiene diez dispositivos y entra a través de un router, y todo va a través de Tor, entonces todos estos dispositivos pueden [derramar] algo muy específico suyo - de usted - a través de los nodos de salida.

Ahora, esto no era un modelo [inaudible]. Eso fue un modelo [inaudible], pero eso no fue tan grave como lo es hoy, porque hoy sabemos que hay un [inaudible] global a través de Internet. Eso significa que cuando se tiene un [inaudible] global de la red, que hace que sea mucho más difícil para la red de anonimato operar de una manera en que tenemos cierto porcentaje de garantía de que usted es totalmente anónimo. En este caso, si tiene varios dispositivos que van a través de Tor que todos [derramar] algo suyo en los nodos de salida, ya que tiene que salir de la red en algún momento.

Tenga en cuenta que es algo que lo podría hacer destacar un poco más. Así que esta es la razón por la que el navegador Tor, por ejemplo, intenta hacerlo lucir como cualquier otro usuario del navegador Tor, para que nadie le pueda sacar una huella digital.

DEV ANAND TEELUCKSINGH: Bien. Gracias, David. Veo que Glenn tiene la mano levantada. ¿Glenn?

GLENN MCKNIGHT: Hola de nuevo. Tengo otra pregunta de Satish Babu. Su pregunta es: "¿Qué tan escalable es Tor? Si muchos más usuarios comienzan a utilizarlo y el número de nodos son más o menos los mismos, ¿podría el rendimiento degradarse? Además, ¿hay algo [posible] [inaudible] se puede hacer para salvar esta situación? "

DAVID GOULET: Muy buena pregunta. El escalonamiento es siempre algo que tenemos en mente. En este momento, trabajamos activamente en el

escalonamiento de [inaudible] servicios. Si lo recuerda de esta presentación, conectarse a un servicio oculto es realmente un trabajo muy, muy intenso en la red y también en la criptografía. Se construyen tres circuitos diferentes. Luego se conecta a esta otra persona. Es un montón de criptografía y una gran cantidad de ancho de banda que se utiliza sólo para la conexión.

Trabajamos en tratar de escalonarlo de múltiples formas. Hemos creado el balance de cebolla de [inaudible] programa de privacidad, que es básicamente un programa [GSOC], [Google Summer of Code]. Y el balance de cebolla [inaudible] servicios. Facebook está realmente muy interesado en eso y utilizan las pruebas beta de la misma. [Bajo balance] es una dirección de cebolla a través de múltiples coordenadas.

Pero si nos vamos a la parte de red, si los relés ahora permanecen igual, si nos fijamos en el gráfico de la métrica, aún nos queda un poco de brecha entre lo que se usa y lo que es [inaudible] de usar, pero es siempre un problema.

Si, digamos, nos vamos a 4 millones de usuarios con esos 6,000 relés, lo más probable es que el rendimiento de la red Tor se degrade. La parte más importante es que, como llegamos a más usuarios, deberíamos conseguir más relés - relés rápidos que permitan desde la salida a un punto de entrada que sea poderosamente rápido.

Así que el escalonamiento es una cuestión importante para nosotros. Cada vez que añada algún componente de seguridad de Tor - por ejemplo, sólo para darles un ejemplo, trabajamos aquí para añadir relleno en la red Tor. El tráfico [correlación] o ataque de confirmación tráfico contempla dos partes diferentes de la red y dice: "Oh, usted es

David." Se vuelve mucho más difícil. Pero entonces añade [cargas] a la red. Así que esto siempre está en nuestros procesos de investigación y desarrollo. ¿Puede la red Tor escalonar lo que se agregó? Y ahora mismo no les puedo dar un sí en firme o no, si se hace el escalonamiento o no. Es un proceso continuo constante. Gracias.

DEV ANAND TEELUCKSINGH: Gracias, David. Sólo estoy viendo si hay alguna otra pregunta rápida. Permítanme pido una encuesta rápida a todos nuestros participantes, sólo para tener una idea de esto. ¿Cuántas personas utilizan Tor? Puede utilizar su Adobe Connect para decir sí o no. Adelante, David. Sospecho que son, por supuesto, grandes consumidores de Tor.

DAVID GOULET: Así que la pregunta es, ¿Cuántas personas utilizan Tor?

DEV ANAND TEELUCKSINGH: Bueno, es más una encuesta para el público. Pero puede contestar a esta pregunta, mientras la gente responde.

DAVID GOULET: Ah, para el público. Bien.

DEV ANAND TEELUCKSINGH: Veo que hay dos personas que indicaron que ellos usan Tor. 14 o 15 personas participan en esta llamada. Ahora veo a tres personas.

Excelente. Sólo estoy viendo si hay alguna otra pregunta rápida. A la una, a las dos. Bien.

David, muchas gracias por su presentación. Fue muy, muy informativa. Creo que tal vez lo que vamos a hacer es poner las diapositivas en la wiki y quizás todavía seguir con preguntas de seguimiento. Vía Glenn, probablemente podríamos transmitirle estas preguntas a usted si hay alguna pregunta de seguimiento. Y tal vez, si el Grupo de Trabajo de Tecnología tiene más preguntas, es posible que desee ponerse en contacto con usted. Nos mantendremos en contacto.

DAVID GOULET: Sí por favor hágalo.

DEV ANAND TEELUCKSINGH: Muchísimas gracias.

DAVID GOULET: Haga preguntas, hágalas publicas. Con gusto.

DEV ANAND TEELUCKSINGH: Genial. Muchas gracias, David. Bueno, ya nos pasamos cuatro minutos. Tenemos otros temas en el orden del día. Yo sólo voy a pedir tal vez un período adicional de cinco minutos para hablar con rapidez sobre los posibles elementos de trabajo inmediatos, objetivos, políticas [TF] de aquí a la próxima reunión número 55 de la ICANN.

Así que una de las cosas que vamos a ver es las soluciones de conferencia. Ahora, como se recordará, el Grupo de trabajo sobre Tecnología ha discutido [inaudible] sobre soluciones de conferencia que comenzaron en el 2013 cuando la ICANN estaba, en cierto momento, considerando el cambio de Adobe Connect como una solución de conferencia a algo llamado reunión Lucid. Y la discusión en ese momento cuando eso sucedía era que, bueno, si iban a cambiar, probablemente deberíamos tener algo que decir en cuanto a qué tipo de solución de conferencia queremos.

Eso comenzó un proceso en el que empezamos a revisar las soluciones de conferencia. Cuando la ICANN parece alejarse de cambiar de Adobe Connect, también paramos de revisar las soluciones de conferencia. Pero he de decir que en la reunión de Dublín - y tal vez, Glenn, usted podría intervenir en esto porque ha tenido una conversación con el personal de ICANN sobre esto.

Algunos miembros del personal de la ICANN hablaron sobre, bueno, utilizamos Adobe Connect, pero buscamos alternativas, Glenn, ¿el resumen es correcto?

GLENN MCKNIGHT: Seguro. Sí. Hablé con Pablo [Hoffman] y él estará presente en nuestra llamada ya sea en enero o febrero y se centrará en la comparación de las mejores prácticas. Hicimos una llamada la semana pasada en la reunión [Flick], que fue una llamada que tuvo mucho éxito entre los participantes. Si hay alguna herramienta de conferencia, la comunidad puede recomendar algo que se aleje de Adobe, entonces, lo que está diciendo es que estamos viendo otras alternativas. Así que por favor

denos una solución. Estaremos encantados de hacer una llamada independiente que muestre esas alternativas. Queremos asegurarnos de que la accesibilidad funcione bien. La gente en todas las plataformas, en Linux, [DSD], móviles. Queremos asegurarnos de que funcione también en países que tienen un ancho de banda lento. Así que tenemos algunos desafíos.

Por favor, si tienen alguna solución, háganoslo saber. Tenemos en nuestro sitio, una comparación de las diferentes herramientas y también tengo una presentación de diapositivas que proporcioné que es un poco anticuada, pero sigue siendo una herramienta muy valiosa desarrollada [con IEEE].

Tiene la palabra, Dev.

DEV ANAND TEELUCKSINGH: Gracias, Glenn. Sólo para responder a una pregunta de - bueno, yo no sé quién, pero a partir de C2 en el chat se habló de mover algo que [inaudible] no sea Adobe y eso sería bueno. Tenemos algún tipo de comparaciones de características. Propusimos un conjunto de características que nos gustaría ver en las soluciones de conferencia. Es probable que no tuviéramos tiempo para entrar en todas las características individuales, pero voy a poner algunos enlaces en la lista Grupo de Trabajo sobre Tecnología, como cuáles son las principales características que buscamos - multi-plataforma, la accesibilidad como lo mencionó Glenn, ese tipo de funciones. Debe tener la capacidad de ver a los participantes, será capaz de solicitar un turno para intervenir de forma que podamos tener una cola para los ponentes que desean hacerlo y así sucesivamente.

Tenemos una lista de características que buscamos. Una vez más, por favor, publíquenlo en el chat o en la lista del Grupo de trabajo sobre Tecnología o algunas ideas que querríamos ver. Así que esa es una de las cosas que queremos centrarnos en entre hoy y la reunión 55 de la ICANN, que tendrá lugar en Marrakech, en mes de marzo. Estamos a mediados de noviembre, por lo que realmente tenemos diciembre, enero, y febrero.

Una de las otras cosas que probablemente podríamos querer mirar es, bueno, tenemos dos proyectos que fueron inspirados por el trabajo en el TTF y los libros electrónicos y subtitulaje. Tal vez podamos dedicar un poco más de atención a esos proyectos. Esos proyectos fueron aprobados por la ICANN y ya son dos proyectos formales que ya han despegado desde la reunión en Dublín y en lo sucesivo.

Glenn, ¿desea mencionar muy rápidamente la idea del libro electrónico?

GLENN MCKNIGHT: Seguro. Maureen y yo hemos estudiado arduamente un montón de diferentes herramientas de [libro de escritura] a [inaudible] y el uso de Caliber para la conversión. Probamos con el Kindle y el iPad. Les tendremos dos libros electrónicos para demostración muy pronto. Vamos a hacer uno de los [inaudible], en parte, con el piloto de subtitulaje en una de nuestras llamadas en el futuro. En realidad es un proyecto interesante porque lo que tenemos es una historia de hacer seminarios en línea con capacidad para construir, pero eso es todo. Sólo unas pocas personas participarán. Esto nos dará aún algo más allá de los

seminarios en línea. La idea es proporcionar a lo largo del eco-espacio. Será un interesante y breve seminario en línea.

DEV ANAND TEELUCKSINGH: Bien, excelente. Gracias, Glenn. Esa es probablemente la segunda parte de lo que tenemos que mirar. En cuanto a las recomendaciones de ATLAS II, sé que - creo que va a haber algunos pasos a seguir para la implementación de ATLAS II en términos de cómo vamos a hacer esas recomendaciones porque ya se ha realizado un montón de trabajo por parte el Grupo de Trabajo sobre Tecnología y otros grupos, sobre estas recomendaciones.

Probablemente vamos a revisar una y [inaudible], posiblemente, ver alguna expresión de interés sería - mirar otros mecanismos de participación que estén en una de las recomendaciones.

Por ejemplo, una de las recomendaciones que alguien había señalado fue mirar las cosas como una retroalimentación líquida y así sucesivamente. Realmente no hemos tenido la oportunidad de verlo en cualquier forma, como tal. Yo no sé si es... Sé que Jimmy ha tenido alguna experiencia en Retroalimentación Líquida y creo que de hecho recomendó que mejor no lo hiciéramos. Probablemente fue una de sus recomendaciones. Pero sí necesitamos al menos entenderlo, así que al menos podemos decir: "Bueno, estas son las razones por las que no aplica."

Probablemente no necesitamos hacer mucho más trabajo para recomendación ATLAS II porque creo que realmente tenemos todo a la

mano, pero por supuesto que cualquiera en el grupo puede no estar de acuerdo y sugerir que tenemos que trabajarlo más.

¿Cualesquiera otras ideas propuestas para el TTF? A la una, a las dos.

De hecho, hay una cuestión más que quiero plantear, en realidad. Todavía queremos catalogar algunos de las cuestiones sobre tecnología que la comunidad At-Large tiene. Empecé a construir eso en nuestro espacio de Grupo de trabajo sobre Tecnología para rastrear las cuestiones sobre tecnología.

Por ejemplo, para Adobe Connect, hubo un problema con respecto a los correos electrónicos principalmente de los usuarios que utilizan direcciones de yahoo.com. Rebotaban de la lista de correo electrónico. Así que quiero rastrear esos tipos de problemas con los que la comunidad se enfrenta y luego planteárselo al personal para poder ver si podemos llegar a - bueno, identificar el problema, llegar a soluciones temporales o en coordinación con el personal de la ICANN. Así que ese es otro elemento de trabajo inmediato para el TTF entre hoy y la reunión 55 de la ICANN.

Una última cosa. Quiero invertir sólo tres o cuatro minutos. Tiempos alternativos para las llamadas del Grupo de trabajo sobre Tecnología. Normalmente, el Grupo de trabajo sobre Tecnología se reúne por lo general un lunes, por lo general el tercer lunes de cada mes a las 15:00 UTC. Ahora, lo que algunas personas han dicho - principalmente aquellas en las regiones de Asia y el Pacífico - es que probablemente este sea un momento muy inapropiado para participar en las llamadas del Grupo de Trabajo sobre Tecnología.

Sólo quiero planteárselo al grupo. ¿Deberíamos tener tiempos alternativos para las llamadas del Grupo de trabajo sobre Tecnología. ¿Queremos alternar las llamadas del Grupo de trabajo sobre Tecnología a manera de ensayo, sólo para ver? Cuando digo un momento diferente, hablo de - Intento recordar cual fue el tiempo sugerido. Creo que fue algo alrededor de las 21:00 GMT o 22:00 UTC. Eso lo pondría a primera hora de la mañana en la región Asia-Pacífico. ¿Alguien tiene alguna idea o comentarios inmediatos sobre que, en cuanto a si se deben tratar estos tiempos alternativos?

Veo a alguien a escribir en el chat. También veo a Maureen a escribir en el chat. De acuerdo, vamos a tratar de tiempos alternativos. Maureen está escribiendo. Mientras que escriben, Glenn, adelante. Tiene usted la palabra.

GLENN MCKNIGHT: Sí. Una de las cosas, las personas, de las que hablamos es porque tenemos tan pocos... Y yo aprecio que Maureen esté en la llamada del día de hoy. Todos sabemos que probablemente sean las 3:00 de la mañana para ella. Definitivamente nos queremos poner en contacto con APRALO y tener una llamada que también sea a muy bueno tiempo para ellos. Yo mismo o Dev, yo estaría encantado de presidir la reunión. Necesitamos un copresidente en esa llamada en la zona APRALO. Si podemos encontrar... Nos gustaría estar en la próxima llamada con APRALO para plantearlo como un problema. Pero creo que hay muchas cosas en las que la gente de APRALO puede participar. Sí, estaremos encantados de dar cabida a otras zonas horarias. Tiene la palabra, Dev.

DEV ANAND TEELUCKSINGH: Muy bien, perfecto. Gracias, Glenn. [Inaudible] lo que dice. Creo que sin duda estamos dispuestos a cambiar a un horario alternativo. Probablemente sólo hacer una rotación de horarios. Podríamos traer a más personas, en especial de la región de Asia-Pacífico. Tenemos un montón de gente que ahora se enumeran de la región Asia-Pacífico, pero que no están presentes en las llamadas. Tal vez por el cambio de horario, podríamos conseguir más de esas personas.

Tal vez lo que podemos hacer es, probablemente, planteárselo a la APRALO. Tal vez entonces tendremos una encuesta Doodle para escoger el momento oportuno y ver a dónde vamos a partir de allí. Para Maureen en este momento son las 5:00 PM.

¿Cualquier otro comentario o cualquier otro asunto?

Sólo por mencionar, también, en cuanto a la interpretación y así sucesivamente, para cualquier otro grupo de trabajo, por lo general la forma de interpretación está a cargo - y el personal me puede corregir en esto - por lo general tres o más personas tienen que solicitar la interpretación antes de una sesión, y tenemos que solicitarlo con por lo menos 72 horas a tres días de anticipación, porque, obviamente, se necesita tiempo para organizar si los intérpretes estarían disponibles para esa fecha y hora. Así que necesitamos al menos tres personas que soliciten una traducción y para un idioma en particular. Así que eso es algo que hay que tener en cuenta.

Sé que hubo algún comentario que debemos tener - Creo que era de Internauta Venezuela que esta sesión debería haber sido interpretada. Pero lo que vamos a hacer es traducir la transcripción de la presente llamada para que esta sesión se pueda leer en español y francés.

No veo más comentarios o preguntas. Y sé que ya nos pasamos 18 minutos después de la hora. Fue realmente una sesión informativa. Gracias de nuevo a David por su presentación sobre los proyectos de Tor.

Me gustaría darles las gracias a todos. Por favor interactúen con nosotros en la lista de correo electrónico y se suspende la sesión en esta llamada. Gracias y que tengan un maravilloso día / tarde / mañana. Adiós.

TERRI AGNEW: Una vez más, la reunión se ha levantado. Muchas gracias por su participación. Por favor, recuerden que deben desconectar todas las líneas restantes y tengan un maravilloso resto de su día.

[FIN DE LA TRANSCRIPCIÓN]