……. Y me gustaría recordarles que por favor tomen sus auriculares dado que vamos a tener un orador en francés. Gracias por asistir, me gustaría presentar a Nii Quaynor que va a ser el moderador del Foro de hoy para el Abuso del DNS y vamos a tener tiempo para preguntas y respuestas entre los paneles. Por lo tanto, si tienen preguntas, identifíquense, digan sus nombres para facilitar la tarea de los intérpretes y los transcriptores.

Nii Quaynor: Gracias. Comprendo que vamos a decir nombres simples y lo vamos a hacer a la manera de internet. Y esto cada vez es más desafiante en tanto que otros comienzan a buscar maneras de no utilizar internet de la manera correcta.

Entonces se comienzan a crear una serie de desafíos o abusos y es importante para nosotros tomarnos un momento y al menos reflexionar especialmente un ambiente en desarrollo como nosotros tenemos. Simplemente en casos en que haya observaciones o desafíos que descubramos y que pueden enriquecer nuestro conocimiento global en cuanto al abuso del sistema de DNS.

Para ayudarnos a comenzar con nuestra discusión, tenemos un panel muy bueno, muy diverso, que tenemos dos secciones de trabajo. La primera parte va a considerar los últimos desarrollos en la lucha contra el sistema de nombres de dominio. Y luego vamos a volver con la segunda parte para tratar los temas de evolución de los fraudes a los nombres de dominios y las posibles acciones y las formas de responder a los abusos que puedan surgir.

Lo que vamos hacer entonces, como siempre, es darle a los panelistas de darles la posibilidad de hacer comentarios iniciales y luego vamos a escuchar y a hacer las preguntas pertinentes para que los panelistas respondan y que esto sea un poco más interactivo e interesante.

Para la primera sesión que es, los últimos desarrollos en la lucha contra el abuso del DNS, tenemos un panel que se compone de los siguientes oradores.
Pierre Dandjinou, Fredirick Gaudreu, Gary Kibby que está ocupado pero que seguramente ya estará en camino y para comenzar entonces, le voy a dar la palabra a ACHARI y si quieren más detalles sobre los oradores en cuanto a su información bibliográfica, creo que ya está disponible en el sitio web. Así que no lo voy a nombrar yo.

Larry tiene la palabra. Gracias.

Larry Ajayi: Buenas tardes a todos. Mi comentario va a ser sobre un estudio de custodia de datos en Nigeria. Y hemos tenido diferentes desafíos de ciber seguridad en Nigeria y estamos tratando de resolver y al hacer esto les voy a mostrar una lista que ya está mostrada en la pantalla sobre los desafíos de ciber seguridad más comunes que ya conocemos.
Esto no es particular de Nigeria, sino que estos son algunos de los desafíos que estamos enfrentando en internet.
Tenemos la suplantación de identidad, el spam, los mails fraudulentos, robo de identidad, denegación del servicio, acceso no autorizado, terrorismo cibernético y virus.

Nigeria, existe la percepción de que Nigeria es quizás el cuartel general de los delitos cibernéticos en el mundo. Esta es la percepción mundial. Pero me gustaría decir que alguno de los desafíos que vemos aquí en realidad no provienen de ahí. Podemos admitir que somos culpables de algunos de ellos, pero no de todos.

Por ejemplo, el spam, si somos responsables, es responsabilidad de Nigeria de terne spam y también reconozco la responsabilidad de los mails fraudulentos. Hay una serie de actividades que se llevan a cabo en Nigeria, son actividades de suplantación y robo de identidad, de lo cual también somos responsables. Pero no voy a aceptar y me declaro inocente de delito de denegación de servicios. Nosotros no lo hacemos, nosotros no somos hackers, porque incluso si lo quisiéramos hacer no tenemos la tecnología para hacerlo.

No somos responsables del ciber terrorismo así que no me declaro culpable por eso y no nos sentimos incómodos con eso porque simplemente no tenemos los recursos necesarios y tampoco mandamos virus. Somos más bien víctimas de virus que vienen de otros lados. Así que bueno, quería aceptar algunas culpas pero otras no.

Y por estas cuatro cuestiones de las que somos responsables si tenemos penalizaciones por estas actividades en la internet, en algunos casos se bloquean las IP de Nigeria y no se aceptan tarjetas de créditos en algunos casos.

Y también descubrimos que en eventos como este, uno quiere hablar como por ejemplo o chatear con alguien o tratar de hacer amigos, quizás el tópico de discusión más general tiene que ver con las estafas o los fraudes, las listas fraudulentas. Que son algunos de los temas más típicos o de consecuencias más típicas de lo que sucede en internet.

Hace algunos años, una de las ciudades de los países europeos fue víctima o cayó dentro de las manos de un ataque en Nigeria. La Embajada interactúo en esto y se pidió o demandó al Embajador de Nigeria en ese país que actuara. Y por lo tanto, hubo una amenaza de muerte para el Embajador, lo cual fue muy serio este fraude en internet. Como país tenemos que actuar y tenemos para esto dos opciones, una opción es declarar la guerra contra nuestro país o matar al Embajador. Y la otra opción, es permitir que el país tenga el derecho de hacer justicia y ponerse a trabajar al respecto.

Dejamos que la justicia de ese país actuara y luchamos contra el crimen o delito cibernético en ese país. Y cómo lo hicimos? Bueno. Se estableció un grupo de trabajo contra el delito cibernético del cual tuve el privilegio de ser parte. Y el grupo trabajó arduamente y resolvimos unas series de intentos de soluciones para lidiar con esta problemática.

Una fue desde el punto de vista legal. Consideramos el punto técnico y el punto de vista de política. Es decir, hubo varios ángulos a considerar. Desde el punto de vista legal nos dimos cuenta de que no había legislación contra, por ejemplo, el fraude de emails, así que tuvimos que tratar algunos de estos temas y desarrollar un proyecto de ley que fue redactado por este grupo de trabajo y que trataba de cubrir los temas de fraude de correo electrónico y ahora, una vez que el proyecto de ley se apruebe y se transforme en ley, porque ahora está siendo tratado por el Parlamento. Va a ser legal, para las agencias de cumplimiento de la ley puedan intervenir en este tipo de transacciones actuales.

Las evidencia o la prueba electrónica todavía no se considera y no se considera prueba por la ley. Y hay una serie de personas que fueron arrestadas. No podemos obviamente condenarlas porque sólo esa

evidencia está disponible como delito cibernético y esto es generalmente una evidencia electrónica que no es aceptada por las Cortes nigerianas.

También, creemos que la industria y los operadores están proporcionando servicios para poder evitar esto y tenemos un mandato para los diferentes miembros y partes para que no sean chantajeados.

También estamos implementando educación en todo esto. Describimos que estos estafadores se ganan la simpatía de las personas que los rodean porque las personas no son conscientes de las implicancias que tienen en la economía nacional.

El argumento es que se puede luchar contra el crimen o el delito en Nigeria y que esto no afecta la economía, pero también le lleva tiempo al público aprender de esto. Por lo tanto, estamos enfatizando la educación pública y la conciencia pública en todos estos temas.

Y los más importante de esta discusión está relacionada con los nombres de dominios. Notamos que muchos de estos delitos cibernéticos, que mencioné anteriormente, no pueden llevarse a cabo sin utilizar el nombre de dominio de una u otra manera. En la mayoría de los casos estos delincuentes clonan el sitio web del gobierno nigeriano y lo hacen porque muchos de los Ministerios de Nigeria y los Departamentos no tienen seguridad sobre los nombres de dominio de alto nivel. Por lo tanto esto es muy conveniente y apropiado para los criminales para utilizar y para copiar estos sitios webs y clonarlos para cometer muchísimos tipos de delitos.

Por lo tanto recomendamos al Gobierno que la utilización de un ".com.ng" que esto sea obligatorio y creo que esto es lo que sigue ahora. En cuanto a los pasos que tomamos me complace informarles

que el delito cibernético está reduciendo en Nigeria y también ya se dejaron de bloquear nuestras direcciones de IP.
Muchas gracias.

Muchísimas gracias. En realidad (….) se recordó a sí mismo que había sido víctima de un delito de suplantación de identidad. Es una buena (…) Bueno. Entonces desde esta perspectiva me gustaría invitar al siguiente orador Pierre Dandjinou.

Pierre Dandjinou: Muchas gracias. Y perdón por la tardanza.
Soy de (…) y en relación a lo que acaba de decir mi colega, esto está sucediendo también en mi país, porque somos vecinos, siempre estamos conscientes de lo que pasa en Nigeria. Y que esto tiene un impacto en nosotros también en DENIN o en Togo también y resto de las ciudades.
Pero por supuesto mi presentación va a ser una especie de informe breve sobe se ha estado haciendo en África para en realidad combatir este fenómeno.
Vemos realmente que en África, al menos los que toman decisiones, se están interesando en este tema.
Han notado que si bien internet es invasiva, el abuso del DNS es un tema muy importante. Cada vez están más gustosos de brindar recursos para que se puedan tomar las medidas apropiadas y se lleven a cabo las misiones apropiadas. Lo cual es muy bueno.
Nos encantaría tener las estadísticas y hacer una especie de evaluación de operación de los ccTLDs pero desafortunadamente esta información no está disponible.

Como dijo mi colega anterior, sabemos que hay hechos formales que se llevan a cabo en diferentes lugares en distinto momento y se relacionan con la estructura que tenemos en los diferentes lugares. A veces la incapacidad de administrar correctamente algunos de los servidores que tenemos y también todo el tema que tiene que ver con el DNS y DNSsec.

Creo que tenemos que tomar consideraciones serias por parte de África desde la perspectiva profesional y también de la perspectiva de la policía.

Ahora, dado este ambiente que tenemos ¿Qué es lo que se está haciendo? ¿Qué es lo que se logró?

Voy a decir que tenemos diferentes enfoques aquí. Tenemos a los profesionales que son los que han dado parte de la capacitación a los operadores, y ahora hemos comenzado algunos talleres sobre seguridad cibernética y esto nos ayuda a saber o a construir más capacidad y a educar cada vez más a personas que obtienen certificación que les permite luchar o al menos asegurarse de que puedan responder en el caso de la gestión de desastres y que tengan estrategias para esto.

En cuanto a África, la certificación para África o África cert, tiene una iniciativa que es de crear capacidades en los diferentes países y África tiene 54 países con diferentes situaciones. Vamos desde Nigeria, tenemos otra historia en Sudáfrica, otra en Togo y África se dice que es el tipo de iniciativa continental que tiene que implementar varias cosas. Una de ellas por supuesto tiene que ver con la sensibilidad que tengan los que toman decisiones.

Porque es importante que entiendan los temas, a veces no entienden los temas en las regiones donde trabajan.

Tenemos un programa para los creadores de políticas que le permite conocer las diferentes clases de tema de decisiones en ciber-seguridad y también queremos entrenar cada vez a más personas que nos puedan brindar soluciones.

Hasta ahora tenemos unos cinco países que están trabajando en esta certificación y cada vez va a haber más en este tema del ser nacional y la idea es que cada país tenga su certificación de DNS.

África sería el repositorio de lo que yo denomino o de toda la estadística que se necesita para combatir esto.

África por supuesto no sólo va a cooperar sino que también va a trabajar y a cooperar en sociedad con la industria y también hay otros actores involucrados que tienen su propio programa de impacto y ciertamente vamos a trabajar juntos para intensificar la lucha y trabajaremos en los talleres contra el abuso de DNS.

Tenemos planificado hacerlo, África cert está tratando de registrar esto y lo otro que sucede en África es el programa de cumplimiento de la ley. Este es el ÁfriNIC que ha establecido su programa hace tres o cuatro años, y tiene objetivos en el Gobierno, hay funcionarios y abogados cuya finalidad quiere sensibilizar e implementar la correspondiente legislación en los países y es por eso que asistimos a reuniones de cumplimiento de la ley y a los talleres que celebra AfriNIC en este momento. Es decir los políticos y Gobiernos cada vez muestran más interés.

Y esto es algo importante. En la última elección en algunos lugres de África tenemos algo específico, una especie de suplantación de identidad, tuvimos un caso, donde la página web de un candidato fue dirigida a su opositor y bueno, se fue al Comité de elección y se planteó el problema y el Comité dijo “bueno, no sabemos qué hacer”.

Este tipo de situaciones ocurren con frecuencia en África y hay que advertir a las personas al respecto.

Y lo último en cuanto a lo que está haciendo Interpol es lo siguiente. Interpol es bastante activa y trabaja con la policía en el Departamento de política para el desarrollo de capacidades. Tenemos nuestros talleres que son interesantes, debido a la especificidad que presentan y para llevar a cabo las diferentes misiones tenemos especie de sociedades entre la policía y otras partes.

Creo que hay una especie de simbiosis al respecto y también podemos decir que hay una especie de falta de confianza en estos aspectos, por lo tanto necesitamos hablar y asegurarnos de que todas las partes entiendan las tecnologías existentes y estas son algunas de las cosas que están sucediendo en África en la actualidad. Lo cual significa que si, estamos tratando de asegurarnos que esto siga avanzando y creo que son buenas noticias de todas maneras.

Nii Quaynor: Gracias a usted Peter. Hemos visto un caso nacional, hemos visto alguna de las actividades a nivel regional y me complace ver que AfriNIC continúa respaldando las actividades del Cert.

Vamos a salir del continente para ver qué pasa con respecto a la distintas perspectivas y entonces, vamos a invitar a tomar la palabra a Frederick Gaudreau de Canadá.

Frederick Gaudreau: Para los que van a necesitar los servicios de interpretación, les pido que se pongan los auriculares porque voy a hablar en francés.

Voy a darles algunos minutos para que se coloquen los auriculares.

En primer lugar, quiero comenzar presentándoles a la organización que represento, (…) de Quebec cuyo mandato es aplicar la ley en Quebec,

aplicar el código penal, tenemos nuestra cede en Canadá que está dividida en diez provincias y nuestro organismo está encargado de hacer cumplir la ley en Quebec.

Para quienes no conocen la geografía de Canadá vemos que Quebec es la única provincia totalmente bilingüe, entonces es importante trabajar en francés. Por eso trabajamos con la policía y con otras entidades que también hablan francés. Así que ahora después de tres años se creó esta organización para reagruparnos y hacer capacitación e intercambiar información

Hemos creado un punto (…) que no hace lo mismo que Interpol, sino que es una organización que intercambia formación para investigaciones con respecto a los delitos.

Es decir que nuestro punto focal es intercambiar información entre la gendarmería y los oficiales de policía que no reciben información.

Me gustaría mostrarles cierta imagen que salió en Nueva York en 1993 en los últimos años, y aquí en la imagen vemos que en interne uno puede adoptar cualquier identidad, según la imagen que vemos en pantalla. El que hizo esta caricatura realmente era un visionario, porque es por eso que demuestra que los policías tienen realmente un trabajo muy difícil que realizar, porque no saben quién está del otro lado del teclado para saber quién está del otro lado de la pantalla necesitamos tener conocimiento e información. Y para ello hace falta la capacitación.

Y también la asistencia de distintas partes interesadas, operadores de la industria y también de las universidades.

En la próxima diapositiva, vemos un fenómeno que ya tiene varios años. Vemos – no sé si todos lo pueden ver – pero vemos en pantalla algo de Interpol, es el primer documento que fue enviado por un usuario de

internet en Quebec, que estaba justamente involucrando a gente de la Costa de Marfil. Entonces, lo que sucedió fue que hubo alguien que se enamoró de una mujer de la Costa de Marfil y esta mujer lo convenció a este hombre de que apareciera en la cámara web.

Entonces, el objetivo de este hombre era justamente conocer a esta mujer.

Cuando esta persona se dio cuenta de que era el único que podía enviar estas imágenes y no había ningún tipo de retorno después de varios días, después de que él enviaba sus propias imágenes por internet, y estaba prácticamente desnudo en esas imágenes, recibió una notificación de Interpol informándole que debía pagar una multa o de lo contrario estas imágenes serían enviadas a las autoridades correspondientes.

Y estos videos fueron publicados en distintos medios de internet. Porque esta persona de la Costa de Marfil era justamente una delincuente.

Obviamente que este hombre no fue la única víctima de este delito. Si no tenemos colaboración internacional en África Occidental no sabemos de dónde se originan esos mensajes, entonces no podremos identificar a la fuente que los envía y no podemos ponerle fin a este problema.

Por eso en la realidad africana vemos un mayor número de usuarios de internet y el acceso a internet es mayor gracias al mayor ancho de banda. Entonces en la comunidad africana por ende, inevitablemente va a haber un incremento de los delitos cibernéticos.

Va a ser como un tsunami.

Por ello que es necesaria la capacitación con respecto a estas herramientas y por eso es crucial la cooperación internacional.

Nosotros aprovechamos esta oportunidad en este Foro de la ICANN para reunirnos con treinta funcionarios policiales, con expertos, con jueces, expertos en materia legal, para asistir a estos talleres sobre delitos cibernéticos y justamente escuchar cuáles son sus necesidades para poder brindarles una mayor asistencia.

La ICANN hizo posible este Foro, este taller, y los jueces y funcionarios policiales estaban muy complacidos de recibir esta capacitación. Este fue el objetivo de la presentación. Espero que vean cuáles son las iniciativas que se están implementando además de lo que han dicho mis colegas aquí.

Con todo gusto contestaré sus preguntas. Muchas gracias.

Creo que es bueno que tengamos ciertas iniciativas y creo que es muy bueno decirles que la Costa de marfil está comenzando a abordar todas estas cuestiones.

Nii Quaynor: Bueno. Nos vamos de Norteamérica para pasar al Continente europeo. Somos muy afortunados de contar con Gary Kibby del Organismo del crimen organizado en Reino Unido

Gary Kibby: Muchas gracias. Me han dicho desde el principio que debo hablar lentamente en beneficio de las intérpretes y trataré de hablar lentamente y de la manera más clara posible.

En primer lugar quiero hablar acerca de la labor del Organismo que represento y de otros organismos en relación con los abusos de DNS. Y también tengo una suerte de problema operativo porque estamos en un proceso en el cual estamos investigando algunos problemas, y esta es

una oportunidad de compartir con ustedes un área problemática. En primer lugar este Organismos de la lucha contra el crimen organizado, es un organismo que reúne a distintas entidades policiales, entre otras, que se encargan acerca del cumplimiento de la ley en el Reino Unido, entre otras cosas.

Obviamente que nos abocamos al abuso del DNS, y tratamos con delitos graves. Y alguien me preguntó ¿qué son los delitos graves?
En contraposición a los delitos comunes u ordinarios. Pues bien, nos concentramos en ciertos casos, por eso hacemos participar a la comunidad. Quizás ahora tengamos seis, siete, ocho, nueve distintas ICANN, por así decirlo, en términos de representación. Estamos trabajando en formar representaciones con otros organismos de cumplimiento de la ley en todo el mundo. Por ejemplo AfriNIC, estamos trabajando con los registros regionales de internet para trabajar en colaboración con las entidades de cumplimiento de la ley en las regiones donde operan. Tenemos representantes de ICANN, de Asia, de Sudamérica, de África, de Europa – la presencia de Europa siempre fue constante -. Entonces esta colaboración en cuanto al trabajo con la comunidad de ICANN es muy, muy importante.

Ahora vemos que Interpol es un miembro observador dentro del GAC y esto posibilita justamente hacer conocer los puntos de vista de la comunidad encargada de la ley.
En vista del tiempo disponible no voy a entrar en detalle, vamos a ver una enmienda que se hizo con respecto al cumplimiento de la ley en el acuerdo de acreditación de registradores. Tenemos un requisito de averiguación de antecedentes, tenemos un ex funcionario del

organismo al cual pertenezco que es un miembro activo del Equipo revisor de WHOIS que es también una primera instancia para que los organismos encargados del cumplimiento de la ley empiecen a cumplir con su trabajo.

Creo que lo que nos preocupa es la identificación de todo aquello que puede tener un impacto sobre nuestro trabajo y nuestras investigaciones. Y justamente la comunidad y ustedes son quienes identificarán las áreas problemáticas para nosotros.

En este momento etas áreas son los gTLDs, los IDNs, el IPv6. Incluso tuvimos dos funcionarios del FBI y de la RCMP que participaron en el Grupo de Trabajo de ingeniería de internet y pudieron comprender el diseño de la internet del futuro.

Esto es algo importante, porque para los organismos encargados del cumplimiento de la ley este es un desafío global.

Sin duda dentro de la comunidad de la ICANN somos un grupo minoritario. Desafortunadamente en cuanto al cumplimiento de la ley en otros negocios más tradicionales también somos un grupo minoritario. Hay muchas empresas que no comprenden qué es lo que sucede dentro de la ICANN, entonces, necesitamos mejorar o elevar los niveles dentro de todo tipo de trabajo policial.

En este momento hay un área particularmente problemática con respecto a la distribución de software malicioso. Todos sabemos que los delincuentes aprovechan todas las debilidades de los sistemas y los procesos, porque eso es lo que hacen los delincuentes. Ellos quieren ganar dinero.

Entonces, no vamos a ver un montón de aspectos técnicos que no comprendo, eso va mucho más allá de lo que puedo comprender, pero

si estamos hablando de dominios y el hecho de que los delincuentes justamente lo único que hacen es tomar el control de estos dominios. Y esto se ve continuamente, una y otra vez, entre los registradores y no vemos un indicio de colaboración pero lo que si vemos es que el control y el comando de todos estos dominios tienen que estar implementado apenas un par de horas, para que estos delincuentes puedan implementar un ataque malicioso.

Si ustedes fuesen hablantes angloparlantes me dirían ¿a qué se refiere todo esto? Bueno. En realidad nos e refiere a nada, sino que son algorismos automatizados que estos delincuentes están produciendo una y otra vez. Y esto, lo que vemos es que hay debilidades en nuestros sistemas y procesos. Entonces vemos que los procesos para la identificación de actividad delictiva no abordan este problema. Porque obviamente una vez que son identificados y uno tiene un problema recurren al registrador y lo contacta en aproximadamente quince días.

Estas personas solamente necesitan quince horas para funcionar, entonces no tenemos una solución. Nosotros diríamos que desde el comienzo tenemos que hacer una averiguación de antecedentes.

Cuando alguien quiere hacer un registró, por qué quiere registrar tal o cual coas. ¿Cuál es el valor comercial?

Todo esto deriva de un mal WHOIS, de todas maneras el WHOIS está mejorando en lo que a la actividad delictiva respecta. Requiere una cantidad razonable de averiguación de antecedentes. Está mejorando, están aprendiendo porque cuanto más hagamos nosotros de estos organismos encargados del cumplimiento de la ley. Entonces más aprenderán y más responderán.

Con respecto al tema de WHOIS, esto es algo muy importante para el cumplimiento de la ley. También el dinero lo es con respecto a estas registraciones, se hacen pagos con tarjetas de créditos robadas, con dinero virtual.

I alguien tiene alguna idea, es justamente allí donde está el problema, en las debilidades del proceso. Y estas eran las dos cosas que quería decir.

Les agradezco la oportunidad de haber participado en este Foro. Muchas gracias.

Nii Quaynor: Le damos un aplauso a nuestros oradores. Escuché palabras muy importantes, colaboración, educación, que tenemos que crear una comunidad y ahora desafíos al proceso.

Creo que ahora le vamos a dar la oportunidad al público de que presente sus preguntas a los panelistas.

Abrimos entonces la sección de preguntas y respuestas.

Tenemos alrededor de diez minutos para trabajar con (inaudible - 1.20.19)

Sería útil mencionar quienes son.

Steve Del Bianco: Soy Steve de Netchoice. Una pregunta. ¿Puede explayarse sobre las enmiendas específicas del RAA en las cuales están trabajando y cuándo se van a implementar?

Gary Kibby: Creo que el tema de las enmiendas, están documentadas en cuanto a las acciones de cumplimiento de la ley. Ha habido una discusión ayer

entre el GNSO y el GAC y creo que las recomendaciones de alguna manera van a abarcar algunos de los temas del abuso del DNS.
Los delincuentes son parte de la evolución del proceso y tenemos que aprender, que sea lo que sea, el proceso que llevemos a cabo los delincuentes van a estar ahí.
Es una cuestión de compartir de ambos lados las especificaciones y recomendaciones que ya están documentadas. Y que tienen mucho valor estas recomendaciones específicas.

Permítame dirigirme en esta sección.

Margie Milam: Por favor su nombre!

Antoinette Johnson: Soy la señora Antoinette Johnson. En cuanto al abuso del DNS ¿Cómo van a evitar el actual o real bloqueo de las consultas del DNS?

En el caso del país donde provengo tenemos bloques de IP genuinos y no genuinos que son bloqueados para poder restringir el abuso del DNS.

Nii Quaynor: ¿Lanre quisieras comentar al respecto?

Lanre Ajayi: Creo que hemos enfocado esta sección pero que deberíamos esperar al próximo panel para poder responder esa pregunta.

Mi nombre es Mary. Soy de Nigeria. Y quiero decir que las agencias de cumplimiento de la ley son muchas veces obstáculos para la seguridad cibernética y muchas veces esto sucede porque el IP y el registro de

nombre de dominio cuando hay un delito, cuando e busca esa IP puede no ser de África o no puede ser de Nigeria.

Puede ser de cualquier lado, de China, el legado y las direcciones de IP hacen que sea difícil para ellos determinar quiénes están detrás del delito.

El otro problema es que me parece que cuando todo el asunto de esta cosa de hablar de una computadora a otra computadora, nadie pensó cómo lidiar con esto y que habría detrás de todo esto. Entonces, si se quiere luchar contra esto, ya sea del punto de vista de las agencias de cumplimiento de la ley o de otro lado, las direcciones de IPv6 tienen que cubrir las brechas que dejaron las direcciones de IPv4.

No necesariamente puede ser que todos los crímenes provengan de Nigeria.

Esto es lo que han establecidos nuestras agencias de cumplimiento de la ley. Pero el hecho es que no pueden determinar quiénes registran o quiénes son los dueños del IP o de los nombres de dominio.

Y entonces yo instaría a la comunidad de internet a que considere esto. Es decir a ver cómo podemos implementar esto, Incluso si estamos llevando a cabo o estamos implementando políticas de ciber seguridad, o como quieran llamarlas, como dijo el último orador bloquear a las (…) nos llevaría a otros horizontes.

Muchas están bloqueadas debido al proceso del uso del DNS y de las direcciones de IP.

Gracias.

En los comentarios, me parece, y espero que no espere que le demos información de identificación en el DNS.

Mi nombre es Niky y soy también de Nigeria. Quiero hablar porque lo que usted dijo es correcto. Hemos investigado y encontramos que muchos de los crímenes son atribuidos a Nigeria y en realidad no son cometidos por Nigeria.
Y les pediría que tengan en cuenta esto en la internet, alguna de estas cuestiones no son cometidas por Nigeria. Gracias.

Eso es verdad. Pero la forma en que se gana la confianza es a través de la actitud local y sabemos que tenemos que seguir avanzando en este tema.
De modo que si, tiene razón.

Rod Rasmussen: Me gustaría hacer un comentario respecto del tema de Nigeria.
Me gustaría comentar que las agencias de cumplimiento de la ley de Estados Unidos están trabajando arduamente en el tema de Nigeria durante los últimos años. Ha habido muchas operaciones conjuntas e interesantes, han tenido lugar recientemente.
Creo que Nigeria tiene un problema y lo ha tomado muy seriamente y lo que vemos es que muchas personas ahora lo que están haciendo es cometer estos crímenes en otros países y cuando lo sacamos de un lugar se van a otro para seguir cometiendo los delitos.
Hay otros países involucrados también. Pero quiero tomar esto como ejemplo tiene que haber una solución global a este problema.
También tengo alguna pregunta para hacerle a algunos de los oficiales y brindar mi apoyo por el trabajo que han realizado.

Gracias.

Lanre Ajayi: Un momento por favor. Me gustaría agradecer el cumplido, estamos haciendo mucho y creo que lo que hicimos fue admitir que el problema de la delincuencia existe, que si existe la ciber delincuencia y las estafas existen. Y el Gobierno admitió que debe implementar medidas para luchar contra este crimen cibernético y necesitamos la ayuda de agencias de todo el mundo, como por ejemplo del Reino Unido que me dijo que han estado trabajando en Nigeria y los Estados Unidos también. Entonces nosotros estamos colaborando y estamos tratando de mejorar la situación de Nigeria y que Nigeria esté libre de delincuencia gracias a estas agencias de cumplimiento de la ley.

Y quiero decir que no estamos libres de realizar transacciones con Nigeria.

(…) Soy representante de la Fundación de internet, y me gustaría comentar sobre la presentación del señor Larne en cuanto a la exactitud de WHOIS que es importante para que las agencias de cumplimiento de la ley obtengan información.

En Estonia el año pasado, desarrollamos una solución en los registros de dominios, donde cada nombre de dominio está conectado a una persona o compañía que es responsable de este nombre de dominio y más allá de esta persona o compañía, está identificada – es decir, no aceptamos registro anónimos – en los registros de nombres de dominio. Aunque tenemos una poca cantidad de dominios son aproximadamente unos 4 mil. Esta solución quizás se pueda aplicar a nivel internacional porque está basada en las recomendaciones del IFTI y de acuerdo con este grupo de inteligencia financiera implementado, el

marco ya está implementado en más de cien países. Básicamente es ver que se trabaje y de rastrear dinero “on line”, pero también rastrear los protocolos de IP y de obtener información que prueba la identificación de los registradores dentro del registro de los nombres de dominio y nosotros guardamos esta información de identificación en el registro central. Gracias.

Gary Kibby: En cuanto a esto quiero agradecerles y vamos a tomar en cuenta sus comentarios.

Nii Quaynor: Bueno. Gracias por su participación en la primera parte. Vamos a pasar a la segunda parte y esta tiene que ver con los procesos de bajas de los nombres de dominios y debido a ciertos delitos que han pasado de la teoría a la práctica.

En la ausencia de una política uniforme por parte de la ICANN para lidiar con este tema, muchos profesionales y agencias de cumplimiento de la ley y corporaciones privadas se han dispuesto a trabajar para reducir estas bajas.

Los panelistas van a explotar los desafíos asociados con estas prácticas y qué imagen o rol deberían cumplir ICANN en la evolución de las bajas de los nombres de dominios y las prácticas relacionadas con esto.

Quiero también decir, para dejar en claro, que tenemos cuatro presentadores, así que le voy a pedir al señor Michael Moran de Interpol que lidere la discusión.

Michael Moran: Voy a comenzar en francés y veo que todo el mundo entra en pánico y sale a buscar los audífonos y voy a continuar en francés. Bueno, entonces continúo en inglés.

Bueno voy a continuar en inglés Soy Michael Moran de Interpol. Soy oficial irlandés, se habrán dado cuenta por mi acento. Y quiero comentar sobre Interpol y saben que toda esta área que ICANN puede hacer sobre los nombres de dominios sobre lo que se puede hacer en este aspecto y también considerando a los vendedores y a los registradores y lo que ellos pueden hacer con os nombres de dominios, quizás creo que sería bueno comenzar con la idea del señor Joe Public va – porque alguien le dijo- va y busca en el WHOIS de dónde viene el nombre de dominio y quién es el responsable. Y eventualmente encuentra esta información y se ve yendo a una página de soluciones de red porque hay una compañía que vende este dominio, entonces él llega ahí e intenta encontrar dónde en este sitio web él puede ir e informar que tiene un problema con un producto que fue vendido por esta compañía.

Entonces va y atraviesa toda esta cuestión y sabe que puede comprar todos los nombres de dominio y que puede tener un 40% de descuento en los certificados y entonces, lo puede hacer porque hay un período de registro que está disponible. Entonces lo que hace es buscar y encuentra y no encuentra el abuso en ningún lado. Entonces trata de contactar a la compañía y es aquí donde él encuentra todo lo que necesita porque hay soporte para el cliente, pero sin embargo, no puede encontrar nada sobre nada. En realidad no puede encontrar nada de nada.

Así que decide continuar con su búsqueda y lo llama a su hermano Peter Public y Peter decide que él va a ir al Presidente de la compañía y decir que tiene un problema y se encuentra en la página de esta compañía, que se llama Enom, e Enom quiere vender este servicio para ayudarlo a Peter a solucionar su problema, entonces él va a la página de INON y cuando llega al final de la página, ve que hay una jovencita muy linda, y hay mucha gente vendiendo, que venden los pluggin de IP, entonces va a la parte final de la página y eventualmente él ve y llega que hay un informe sobre abuso del DNS. Muy bien, muy bien, felicitaciones.

Entonces dice, yo quiero informar el hecho de que fui víctima de un abuso por parte de mi cliente y entonces lo que hace es, va a informes y se da cuenta que no encuentra el informe, y entonces ve que también hay pornografía infantil, usurpación de identidad, pero recibe algo de spam. Pero al menos tiene algo para reportar porque cuando él va a su primo que trabaja en Afilias, Afilias tiene un problema con GoDaddy que es una maravillosa compañía y que tiene muchísima gente contenta que vende muchísimos lindos productos y nunca vamos a criticar a una compañía que hace dinero porque en realidad eso es lo que hacen las compañías. ¿Entonces qué hace él? El avanza, sobrepasa a toda esta gente tan brillante y tan buena, y ve que llega ahí y que no puede avanzar con su informe. Y dice: uy caramba! Hay un informe de spam, pero yo lo que quiero reportar en realidad, no es un problema de spam sino de “maleware” o uso indebido. ¿Entonces él qué hace? Entra al informe de spam y completa ahí su nombre, su dirección y dice: bueno, ¿Vamos a reportar una usurpación de identidad? Él puede reportar y reportar spam de los foros spam, de las salas de chat spam, de email y llega a la última parte y ve que hay una pestaña que dice “misceláneas” Muy bien GoDaddy, perfecto!

Pero también se puede reportar o informar la suplantación de identidad, se puede reportar o informar pornografía infantil, pero lo que quiere no, entonces quizás, lo que yo trato de decir aquí y quiero hacerlo rápidamente, porque tengo poco tiempo, es por qué es que algunas compañías no hacen informes en absoluto y por qué es tan difícil encontrarlos y algunas otras compañías, sólo hacen informe de spam o intentan simular que lo hacen, porque por ejemplo trabajan en Afilias o porque trabajan con seres humanos y son seres humanos inteligentes y saben que se puede informar.

Y tengo que preguntar por qué solamente se informa el spam.¿ Por qué no se puede informar el abuso de manera normal?

¿Por qué no se puede? Perdón voy a bajar la velocidad. ¿Por qué no se puede reportar el spam de la manera normal? O el abuso, de la misma manera que se reporta o se informa el spam, en lugar de atravesar todo el proceso que describí al principio.

Es una cuestión de interés o es simplemente una cuestión de salir de la idea principal de lo que señala el RFC 2142.

Seguramente ya lo escucharon a este señor mayor que habla al respecto. Steve y Dave son dos personas mayores que están fumando ahora una pipa en algún lado, pero si buscamos la palabra abuso vemos que hay una serie de temas y uno de estos es que los dominios deben tener un ".abuso" o "."lo que sea. ¿Para qué? Para informar la conducta inapropiada.

Y yo acepto que las compañías tengan que poner recursos en esto, Espero que haya una cantidad importante o espero al menos que las haya.

Bueno. ¿Qué vamos a tomar hoy? ¿Qué voy a comer hoy?

Bueno se está acabando el tiempo, vamos terminando entonces.

¿Por qué entonces? Volviendo al tema. Porque las compañías de la que yo les hablé hoy son las tres compañías más importantes y están de alguna manera violando el espíritu de esta RFC. Si uno tiene diferentes categorías, tiene diferentes revendedores y actores más pequeños, la acción debe comenzar desde el comienzo. No sólo así, sino que hay que crear una percepción. Si uno tiene un problema en internet, es un problema de uno, porque seguramente no es mi problema. Pero hay que tratarlo.

Muchas gracias.

Nii Quaynor: Muchas gracias. Eso fue muy elocuente. Muy claro. Me gustaría invitar ahora a Rob Rasmussen del grupo Anti suplantación de identidad de los Estados Unidos.

Rod Rasmussen: Voy a hablar acerca – o voy a seguir esta (inaudible -59.06.6) que mencionábamos antes así que ahora voy a hablar de algo completamente diferente. Es algo que ustedes escucharon antes y es el abuso o el proceso de suspensión para la resolución para el abuso de los nombres de dominio o vamos a crear el acrónimo ADNRS, como se hace en la ICANN.

Para los que no los conocen aquí la idea es tener una manera confiable para que la gente que trabaja en el cumplimiento de la ley o quienes trabajan con la suspensión de nombre de dominios, por ejemplo bancos, profesionales de la seguridad que lo hacen todo el tiempo, tengan una manera confiable para que los registros interactúen con

ellos de manera precisa y controlada, para crear un sistema confiable para la suspensión de los dominios.

Entonces esto llega al nudo de todas las cuestiones que hemos enfrentado en los últimos años y que ayudan a que las personas interactúen cuando se trata de una suspensión de un dominio y para que haya mayor escalabilidad y uno trabaje con gente confiable a gran escala. Y se pueda repetir un proceso que también se pueda auditar.
Esto intenta lograr una madurez en la industria y esto se hace estrictamente para los dominios registrados por delincuentes, no es para suspender dominios que simplemente estén comprometidos.

En el caso de suplantación de identidad, vemos que el nombre del dominio ha sido (hackeado) o también hay otro componente del sistema que ha sido (hackeado), entonces, no es el nombre de dominio lo que se va a suspender, solamente esto se aplica a los dominios registradores y en posesión de los delincuentes.
Les voy a dar una serie de indicadores que nos dicen que se trata de este tipo de este nombre de dominio. Son parte del proceso de informar la suspensión del nombre de dominio está clara aquí.
Vamos a ver que esto agrega bastante riesgo a quien quiere suspender el nombre de dominio y a la otra parte, el registro y el registrador por ejemplo.
Esto ha sido siempre un problema que consterna a todos. Y es la razón por la cual estamos haciendo esto.
La clave aquí es que queremos que estos sistemas sean remplazados y tener un modelo en el cual podamos ampliar el tema de cómo abordar los abusos o en una manera que podamos confiar en la comunidad y

avanzar más rápidamente de lo que hacen nuestros oponentes. Ahora tenemos barreras que se interponen entre nosotros aunque estamos todos del mismo lado. Tenemos barreras y queremos sortearlas.

Entonces, estamos en el Beta 3.1, creo que la primera vez que presenté esto fue en la reunión de ICANN en Los Ángeles.
Como ven en la pantalla estamos viendo que tendremos una reunión de APWG el mes próximo en San Diego para evaluar el programa.
Es un programa que está en versión Beta, pero es un programa en funcionamiento, se encarga de las suspensiones en línea.
Entonces, estamos trabajando con este grupo, creo que tengo una diapositiva al respecto, se lo voy a decir más en detalle, pero como les dije antes, tenemos criterios específicos.

La gente conoce estos criterios, tenemos mucha documentación para que la gente complete para formar parte del programa para asegurarnos de que sea una parte legítima, que sus empleados también lo sean, que todos sus temas corporativos, financieros y de seguros esté cubierto. Es decir que si hay un problema con una solicitud podamos tener algún tipo de recurso.
Esto es lo que ve un solicitante, tiene un proceso que atravesar cuando presenta una solicitud para pasar a ser usuario del sistema y hay arios roles desempeñados. Hay un comité en el APWG, en este grupo de trabajo contra suplantación de identidad para que los expertos en la materia trabajen en esa organización y estudien, mejor dicho, a esa organización.
Esto es lo que vemos con respecto al software y se ha mejorado en los últimos años y ya está prácticamente listo para ser lanzado.

Aquí vemos como se ve una solicitud, hay que ingresar el dominio, el URL completo y el nombre completo del página web. Hay que tener dos requisitos muy altos, por ejemplo con contenido malicioso y la falta de contenido legítimo pero hay que demostrarlo. Se firma electrónicamente y luego se envía la solicitud de suspensión de la resolución del nombre de dominio. Aquí vemos como se ve, esta verificación, aquí tengo los distintos criterios y esto nos permite rastrear muchas estadísticas para ver qué está sucediendo y qué es lo que se suspende o cuáles son las solicitudes de suspensión, es decir que impulsa mayor investigación que podemos hacer como comunidad, para abordar esta cuestión.

No solamente desde el punto de vista de una investigación, esto es lo que vería un registro; ingresan la solicitud y luego pueden decidir cuál será el proceso para abordar con una solicitud en particular, ya sea hacérsela llegar a un registrador porque quizás tiene una relación comercial con el (registratario), pero esto lo enfocamos a nivel de registro pro el tema de la escalabilidad. O sea que es un proceso de ida y vuelta.

Bueno, me estás diciendo que me queda un minuto para terminar la presentación; así que voy a ir un poco más rápido.

Tenemos un sistema de rastreo aquí, ambas partes pueden saber qué es lo que está sucediendo y ver el status de distintas solicitudes y esta es la última diapositiva de mi presentación, así que termine a tiempo.

Entonces el resumen, tenemos un sistema que es riguroso, escalable, auditable y que también puede hacerse rutinariamente.

Queremos tener más miembros de este programa, en versión Beta, tenemos siete registros, dos TLD que están interesados en el programa, en participar directamente en el programa y algunos de ellos no lo han hecho público, así que nos los puedo nombrar aquí, pero hay al menos un par que son bastante importantes. Sé que hablé con muchos registros en los últimos años, que no están en esta lista, pero que se han manifestado o que han manifestado su interés. Así que si son registros o incluso registradores por favor, escríbanme a mí o a Peter (…) al respecto.

Muchas gracias.

Nii Quaynor: Gracias.

Bien. Vamos a pasar a Don Blumenthal del Registro Público de internet de los Estados Unidos.

Don Blumenthal: Gracias. ¡Qué milagro no tengo diapositivas! ¿Qué pasó?

Cada vez que voy a clase, mis alumnos se ponen locos cuando no tengo las diapositivas

Estoy aquí en representación del interés público y también quiero hablar acerca del rol de la baja de los nombres de dominio.

Esto significa que tenemos que lograr que las entidades encargadas del cumplimiento de la ley, se encarguen de dar de baja a un determinado nombre de dominio. A nosotros nos interesa trabajar con las entidades encargadas del cumplimiento de la ley, justamente esto se refleja en el nombre de mi entidad, es el registro que se encarga del interés público, es el registro de interés público en internet.

Entonces queremos asegurarnos de que se haga lo correcto. He trabajado en el cumplimiento de la ley durante muchos años, pero creo que al ver estas cuestiones, es importante de tratar de definir ciertos términos.

Hablamos acerca de la baja de un servidor, de la suspensión, del dominio, del re-direccionamiento, del bloqueo, del filtro, de un dominio y otras series de términos que se utilizan en el campo de cumplimiento de la ley en el mundo de internet.

Parte del rol que podemos desempañar o por lo menos que yo puedo desempeñar aquí es sugerir que todas estas técnicas tienen diferentes fortalezas y debilidades. El factor crítico en toda acción de cumplimiento de la ley en internet es sacar el contenido de ese tema para asegurarnos que no esté disponible y hay determinados momentos en los cuales este re-direccionamiento o la baja directamente no es la mejor opción. En un mundo ideal haríamos lo que hacíamos en los primeros días cuando teníamos la FDC, le decíamos a un juez que resuelva se de baja a tal servidor, eso era muy sencillo cuando el servidor y el juez estaban en el Estado de Virginia, en un radio de 50km.

Obviamente esto ya no es posible porque rara vez puede volver a suceder. La gente ahora muy inteligentemente utiliza distintos dominios de alto nivel, y va dispersando el contenido para evitar este tipo de acciones, pero cada una de estas medidas tiene sus fortalezas y debilidades y tiene efectos auxiliares potenciales.

A veces hay que ver la solución ¿O los efectos colaterales son peores que la solución?

Ahora hay un debate en los Estados Unidos con respecto al re-direccionamiento. Re-direccionar el tráfico en internet puede ser de

mucha utilidad en alguna situación, pero no en otras. Sobre todo en cuanto a propiedad intelectual, habrá quien tendrá un incentivo para evitar una resolución judicial.

Es fácil hacerlo allí, entonces hay que preguntare si realmente esto vale la pena. Por otra parte el re-direccionamiento para ponerle un fin al software malicioso o spam. Bueno no sé cuanta gente tratará de recurrir a esto.

Entonces hay que lograr un equilibrio permanente entre ver cuál es el objetivo y cuál es el mecanismo apropiado en cumplimiento de la ley.

Creo que otra cosa a considerar que se mencionó en otras sesiones, es que hay que tener en cuenta que – o la comunidad de registro, registradores y entidades de cumplimiento de la ley tienen que estar siempre en contacto.

Todos podemos colaborar para utilizar la terminología adecuada para lograr los objetivos necesarios.

Tenemos solamente la mitad de la información para lograr todas estas cosas. Queremos lograr esto, pero sin embargo, tenemos que volver a ver a nuestros fiscales y decirles “tienen que volver a redactar tal o cual cosa porque no están utilizando la terminología correcta”.

Hace un año más o menos, hubo un incidente en los Estados Unidos, se realizó una baja de dominio en los diez dominios, pero debido a la redacción de dicha resolución cayeron miles de dominios que no tenían ningún problema – 84 mil dominios cayeron-.

Entonces hay que ver la mejor manera de cómo se puede lograr las cosas técnicamente y garantizar la mejor manera de que todo quede bien redactado para no tener estos potenciales efectos colaterales.

Muchas gracias.

Nii Quaynor: Gracias. Creo que vamos a pasar a la última presentación que va a estar a cargo de Titi Akinsamni de la Universidad de Witwatersrand de Sudáfrica.

Titi Akinsamni: Gracias. Bien. Bueno comenzamos. Como experto en tecnologías. Buenas tardes a todos. En interés y de ser breve porque hemos tenido un día largo, voy a hacer una serie de comentarios al final de mi presentación.

Voy a hablar lento para los intérpretes, pero voy a pasar las diapositivas rápido para poder tener tiempo de hacer comentarios.

Entonces. Las bajas de nombres de dominios e incumplimiento de los derechos de internet.

Esto es más o menos, o muy a menudo está relacionado con tener que entender por qué estas bajas son importantes y también se busca en las personas que tienen el concepto de lo que está bien y lo que está mal. Y también está visto desde el punto de vista de las barreras contractuales que existen, o en el caso de los criminales cuando hay que pasar de un campo a otro. En algunos casos cuando en realidad me identidad fue violada o cuando mi tarjeta de crédito se utilizó para algún fin no autorizado.

Al presentar hoy mi tema, voy a hablar de una tendencia particularmente del caso de Sudáfrica. Yo nací en Nigeria y voy a decir "si, hagan negocios con nosotros". Vivo en Johannesburgo y lo he hecho durante los últimos ocho años y voy a hablar luego del concepto de al seguir avanzando y respetar el derecho de libertad.

Y voy a hablar articuladamente del rol que debería cumplir la ICANN.

Se dijo que en 1944 internet era un poco interesante – a veces estoy diciendo que estoy de acuerdo y a veces no – y voy a decir que muchas

veces en inglés se puede aceptar esta palabra como concepto de "fascista".

Particularmente estoy hablando de la baja de el dominio "director.com", me encanta el "soccer" y vi el partido hace unos días, y a veces porque vivo en un país en desarrollo seguramente no puedo tener el acceso a ver estos partidos y tengo que ir a esta página "director.com".

Entonces visité el sitio y cuando no lo podía visitar, visité los foros. Podía tener acceso a todo y me di cuenta que como tenía información y porque tenía suficiente conocimiento se entendió que incluso cuando hubo un caso presentado por el Tribunal español que esto es legal. Pero otro gobierno u otra institución, lo puede dar de baja.

Punto final. No uno sino también el sitio de (inaudible)

No hay más espacios para otros comentarios. Pueden traer al Papa si quieren, pueden traer al Dalai Lama, a quien quieran, pero simplemente les dan de baja. Le dan de baja todo el tiempo y ahí, punto final.

Y luego tenemos el caso de "wikileaks" es algo que yo tomo como una baja por robo. Entonces decimos "dejen de publicar ese contenido" y tengo que ser muy claro. De ninguna manera esto no tiene la idea de estar a favor de este caso de "wikileaks". Esto tiene que ver con otro tema. "Wikileaks" no está bajando esto directamente y me encanta ser como James Bond. Las operaciones de James Bond están relacionadas con el "wikileaks".

Entonces, en los últimos diez o doce, o cinco horas, el fundador de "wikileaks" tuvo que anunciar que tenían que dejar de publicar porque estaban entrando en problemas financieros. Entonces alguien importante, nadie mencionó ningún nombre, ningún gobierno, ningún sector, nadie. Había bloqueado la capacidad de recibir fondos. E incluso

en un sistema básico normal. Y esto es algo interesante. Esto es una forma muy interesante de baja.

Entonces, en el caso de Sudáfrica, que estamos más cerca de nuestro hogar. Los actores electrónicos de Sudáfrica proporcionan protección para los proveedores de servicios de internet. Los protegen pero cuando no actúan estos proveedores no son protegidos y entonces ahí suena la campanita, tin-tin-tin.

Si usted es el proveedor del contenido, no está cubierto y si es el que porta este tipo de contenido por ejemplo el contenido del nombre de dominio, está protegido hasta cierto grado pero en otro grado no.

Pero los que están en el medio y nos volvemos a la conversación que ya tuvimos- o el tema de mi equipo de futbol, no se puede ubicar de ninguna otra manera. Entonces ¿Qué pasa con los usuarios finales que están en el medio de esta situación?

Mientras me preparaba para esta sesión le dije a Maggie que me gusta la legitimidad, y me gusta que las cosas se hagan bien.

Y una de las cosas que hice es ir a la Asociación Sudafricana de Proveedores de internet y solicité información sobre las bajas que recibieron en los últimos años.

La primera pregunta que me hicieron es “¿quién es usted y para que quiere esa información?” y yo dije “bueno, yo soy una usuaria de internet y no me gusta que me hagan este tipo de preguntas”. Necesito esa información y me volvieron a preguntar “¿quién es usted y por qué quiere esa información?”. Y yo tuve que decir “bueno, yo soy un miembro de ICANN”.

Y boom! Ahí estaba la información. Así que funciona decir que uno es miembro de ICANN o de ALAC como en mi caso.

Entonces desde abril de 2005 ha habido muchísimas solicitudes, aproximadamente 284 solicitudes de baja, entonces ¿qué pasa? ¿Qué hacen las asociaciones africanas de proveedores de internet?

Hay ciertos miembros que dicen que si hay una solicitud de baja, seguramente no va s a tener un problema con GoDaddy.

Una vez que uno tiene esta solicitud no queda claro quién es el dueño y si el dueño del nombre de dominio es informado. Entonces uno se puede levantar a la mañana y no poder acceder al dominio o bien, podrá acceder y que a los dos minutos desaparezca.

En el 2010 hubo 148 solicitudes de bajas, entonces mi pregunta fue "¿puedo tener información sobre el tipo de dominio'" y me dijeron "bueno, no sé si podamos dar esa información, seguramente vamos a necesitar que usted se identifique".

Estoy hablando otra vez rápido así que pido perdón.

Entonces, yo otra vez dije "necesito más información" y me dijeron "bueno, en realidad necesitamos más información sobre usted y lo que usted está haciendo" "¿para qué quiere esta información?"

Básicamente para esto se necesita la información.

Entonces. Mi sugerencia es la siguiente. Yo hablo de este punto. Hablo a una sala de gente informada y quiero ser cuidadosa de no atentar o no intentar tocar temas repetidamente. Internet tiene derechos básicos, los derechos humanos llevan al uso de internet.

Y por esto creo que necesitamos tener en cuenta a seis de ellos.

Internet es para todos, y si es para todos tenemos que poder asegurar que se me va a negar el acceso en algunas de las cosas de las que necesito y si es así que se me informe.

Segundo, es una expresión –libertad de expresión – y de asociación, esto requiere más discusión. Y si necesitamos más información de este derecho, por favor consulten la página web de APC.org

En cuanto a los procedimientos en Sudáfrica es algo que quiero mencionar porque creo que tenemos que hablar de lo que ICANN puede hacer.

¿Un minuto me queda nada más?

¿No sé por qué me queda un minuto?

Soy la única mujer que está hablando en forma técnicamente, entonces reclamo que me den más tiempo.

La cuestión es un incumplimiento, una violación, entonces qué tema o qué se toma como abuso.

Una vez que se presenta una acción se tiene que publicar, se tiene que hacer pública y hasta ahora no tenemos información clara de (…) y de la Corte al respecto.

Las partes tienen que ser informadas.

EL tres es que la raíz es donde existen las reglas y cómo se explotan y qué es lo que tenemos que tener en cuenta.

En cuanto a la búsqueda de acceso digo que estas son mis sugerencias. Si estamos buscando una especie de sistema que funcione para las tres partes, es decir, las agencias de cumplimiento de la ley. Quiénes tienen el derecho de asegurar que tengamos seguridad on line?

Y también que aseguren que los criminales sean juzgados y sean juzgado a tiempo y que toda la información sea removida cuando tenga que ser removida.

Y que haya instituciones para los usuarios finales y que también podamos sentirnos seguros como usuarios finales cuando sufrimos una violación.

Entonces esta sería mi pregunta.

En segundo lugar ¿Qué sistema no judicial, pero si legal, nos puede servir como plataforma legal para resolver este tipo de temas?

Yo estoy de acuerdo en que quizás ICANN no tiene que estar relacionada con los contenidos, pero debe ponerse en una situación en la cual estos temas, especialmente lo de las bajas, se puedan tratar. ¿Cómo? Seguramente habría que trabajar y tenemos que tratar de implementar alguna especie de pensamiento colectivo para poder tratar este tema y por supuesto prevenir las influencias negativas.

Les doy dos ejemplos. Una tiene que ver con (…) y la otra es el ejemplo de (inaudible).

Necesitamos buscar un sistema que no sea abusado con facilidad a favor del interés público y privado.

Entonces, en conclusión, me gustaría decir lo siguiente.

Las bajas del DNS es un tema complejo, la industria, los gobiernos que pueden seguir o atravesar y solucionar los temas de las bajas de DNS lo tiene que hacer exitosamente, pero la pregunta es que si yo como individuo, usuario individual, tengo que informar un tema ¿Dónde voy? Esa es la pregunta, esa pregunta no está respondida. Y aparte de esto. Si el caballero que le disparó al Embajador en Nigeria hubiera tenido algún impedimento no lo hubiera logrado.

Nii Quaynor: Muchas gracias. Creo que no tenemos mucho tiempo disponible, así que me gustaría obtener comentarios del público.

Quiero mencionar brevemente que esto es un ejemplo de lo fácil que es pasar por alto algunas resoluciones judiciales.

Realmente todo está accesible en cuestión de minutos.

Bertrand de la Chapelle: Buenas tardes. Soy Bertrand de la Chapelle, miembro de la Junta Directiva de la ICANN. Y en los últimos cuatro años fui representante del GAC por Francia.

Quiero decir que me complace muchísimo ver como se va profundizando el debate. En el último año y medio estuve aquí y en el IGF, todo el debate con respecto al cumplimiento de la ley, veo que es cada vez más y más profundo.

Quiero rápidamente decir dos cosas. Primero, algo para Michael Moran. Valoro mucho su presentación, pero si veo la situación desde la perspectiva del usuario, para poder ir al sitio web del registrador y hacer una queja, uno básicamente necesita entender todo el sistema.

Entonces, hay que ver quién es el que se registró, quién era el registrador, etc.

Una de las preguntas que quiero plantear es ¿Qué clase de debate se llevó a cabo con respecto a otro tipo de actores?

Pienso por ejemplo en el tema de los buscadores o todo lo que utiliza el usuario para que prácticamente sea como un acto reflejo notificar un problema. Quizás es una idea un poco tonta, pero bueno, estoy abierto a sus aportes.

En segundo lugar quiero retomar lo que mencionaba TITI, hubo un problema que ella describió con el tema de la página Royal Director, ese es un problema fundamental, jurídico y de soberanía y tiene que ver con las jurisdicciones.

Hoy nos enfrentamos con el siguiente problema. Cómo hace el Gobierno Nacional “A” y cómo se siente cuando una actividad de un ciudadano de dicho país “A” que es perfectamente legal, conforme a la ley aplicable de dicho país, no puede llevarse adelante en la jurisdicción

del país “B” simplemente porque el nombre de dominio que utiliza esta persona, fue adquirido en un registrador del país “B” o en última instancia supongo el registro del país “B”.
Es decir ¿Podemos formalmente decir hoy que porque “.com” o “.org” son registros con base en la jurisdicción de los Estados Unidos, Estados Unidos y su jurisdicción legalmente son aplicables a toda actividad realizada en un dominio de segundo nivel registrado bajo esos registros?
Esa es una pregunta muy, muy jurídica, legal.

Nii Quaynor: Vamos a – creo que deberíamos escuchar más preguntas –
Vamos a leer una pregunta de un participante remoto.

Margie Milam: ¿Cómo funciona la baja del DNS con DNS entre pares que no tienen control central?

¿Algún miembro del panel podría responder la pregunta?

Rod Rasmussen: Bueno. Supongo que como soy de la comunidad técnica tengo que contestar yo. No funciona tan bien desde el punto de vista de eliminar o retirar un nombre de la raíz o del TLD. Funciona de igual manera, no interesa si es entre pares.

Desde la perspectiva del bloqueo o filtrar eso depende de dónde uno lo esté haciendo. Dentro de nuestra misma red eso no tendrá importancia porque el (…) del nombre de dominio o DNS es el que hace ese bloqueo. Entonces, si el bloqueo o el filtrado se hace (inaudible) probablemente no lo afecte demasiado.

Depende de donde se encuentre usted para ver si el bloqueo va a funcionar y si algo se va a remover por completo.

Michael Moran: Michael Moran. Quiero volver a la observación del señor de la Chapelle. Creo que nosotros en el área de cumplimiento de la ley, estamos desilusionando al público y alguien – un sargento de la policía me decía - ¿Qué pensaría tu madre con respecto a cierta situación?

Entonces si yo veo que estoy perdiendo dinero en ebay, bueno, la madre no sabría qué hacer. Entonces estamos hablando de lo siguiente. El problema es que tenemos a la gente del mundo académico, del cumplimiento de la ley, de la industria, de los derechos civiles, todo el mundo tiene mediciones, pero nadie sabe la magnitud del problema; nadie sabe cuál es la definición del problema.

En un país se define de una forma y luego se define de otra y los informes de delitos cibernéticos se toman en cuenta de distinta manera en los países si es que se los toma en cuenta.

Entonces no podemos considerar cuestiones como las que planteó TITI sin saber justamente la magnitud de las mismas.

Nii Quaynor: Obviamente necesitamos una plataforma para estos informes.

Alejandro Pisanty: Buenas tardes. Soy Alejandro Pisanty, profesor de la Universidad Nacional de México a cargo del Capítulo de internet, también en México.

El bloqueo, el filtrado de los nombres de dominio, comparten muchas características con otras formas de bloqueo en internet que justamente se construyó para sobrepasar el boqueo.

Quiero expresarle mis respeto a Mick Moran y decirle que no me puedo comunicar con él porque Interpol me bloquea el correo de la Universidad, así que tengo que venir desde México a Dakar y viajar miles de kilómetros – 18 mil kilómetros – atravesar capitales europeas para decirle cara a cara que me cae muy bien y respeto su trabajo y otras cositas más, que se las diré en privado.

Los problemas con el bloqueo son fundamentales y es necesario resolverlos. Resolver el problema de la conducta humana que estamos enfrentando, el abuso infantil, el fraude, y todas las consecuencias y ramificaciones. En la sesión del IGF que tuvo lugar en Kenia hace poco, hubo un ejemplo muy, muy bueno.
Un funcionario encargado del cumplimiento de la ley en Australia que describía como se hacía el rastreo de delitos muy graves sobre todo alguien que estaba vendiendo sexo en vivo con menores de edad en internet.

Esta persona era el padre de dos niñas, nosotros no vamos a solucionar este tipo de problemas mediante el bloqueo o el filtrado o creando formas de bloquear, de negar, de autenticar. Nosotros como miembro de la sociedad, como seres humanos, tenemos que concentrarnos en las leyes, las instituciones y la psicología y la sociología de los seres humanos que cometen delitos.
Necesitamos herramientas que sirvan para compensar el efecto de este flujo libre de información para fines maliciosos.

Pero hay que focalizarse en la conducta y cómo implementar todas las instituciones tradicionales. Necesitamos herramientas de nivel 8, una vez que las tengamos entonces vamos a poder trabajar al respecto.
Un Foro como el de la ICANN, como el de la IGF o el de la IPVWG. Todos esos foros nos permiten reunirnos y dejar de discutir entre nosotros y competir entre nosotros y ver cuáles son nuestros objetivos compartidos.
Muchas gracias.

Wendy Seltzer: Soy Wendy Seltzer. Consejera de la Unidad constitutiva de usuarios no comerciales. Y también soy fundadora de un sitio web "chillingeffects .org" que justamente se aboca a reportar amenazas legales y ayuda a los usuarios a entender por qué a menudo los sitios web y otro contenido "on line" no están disponibles debido a las quejas presentadas.
Vimos que Rod habló o se dirigió a usted, porque usted presentaba una herramienta que parece útil para ver el estatus de ciertas situaciones. Usted está pensando acerca de la transparencia y cómo los usuarios de internet y los investigadores como Titi pueden averiguar por qué los nombre de dominios ya no están resueltos o qué ha sucedido con su contenido. O lo que los usuarios pueden hacer para revertir esa situación.
Qué podemos hacer para mejorar la transparencia de las bajas de los dominios para asegurarle al público que se las utiliza solamente en casos legítimos?

Nii Quaynor: ¿Algún comentario por parte del panel?

Rod Rasmussen: Voy a hablar acerca de la última parte de la pregunta. Porque fue dirigida hacia mí. Justamente tenemos un sistema que no tiene demasiada rendición de cuentas, hace todo "ad-hoc" entre personas que se conocen entre sí y se envían los informes y todo se basa en esos informes. La idea de contar con este sistema de APWG es justamente tener estadísticas publicadas acerca del contenido de todos los sitios que han sido removidos. Nosotros trabajamos con miembros del mundo académico y vemos cómo trabajar en toda estas cuestiones. También hay un mecanismo para revertir todo esto, en el sistema, y se puede obtener una retroalimentación inmediata sobre la base de quién está tomando determinada acción. Obviamente que escuchamos a muchas personas como usted planteando todas estas preocupaciones y a nosotros también nos preocupa.

No queremos retirar contenido legítimo o incluso contenido controvertido, porque esto va en contra de cosas sobre las cuales estamos de acuerdo.

Nosotros estamos de acuerdo en ir en contra de la suplantación de identidad y el software malicioso.

Nii Quaynor: Creo que vamos a tomar las preguntas y los comentarios planteados y vamos a responder, vamos a escuchar al último miembro del público y luego responderemos a todas las preguntas.

Tiene la palabra Mouhamet.

Meuhamet Diop: Gracias señor Presidente. Cuando uno ve la cantidad de actores que trabajan en el área de las resoluciones de disputas, en el DNS, el cumplimiento de la ley también, a mí me gustaría dejar en claro dos casos. Los ccTLDs y los gTLDs y los nombres de dominio, lo cual es muy

importante para mí. Y por otra parte tengo dos actores principales en cuanto a la intervención y a la acción. Los entes reguladores y los organismos de la ley, dentro de los cuales uno encuentra a las fuerzas policiales, a los tribunales, etc.

Si vemos el ejemplo del sector de la telefonía móvil porque allí hay mucho dinero, o de los dispositivos móviles, vemos que hay mucha infraestructura para solucionar los problemas. Y es para mí muy grato que uno de los mejores en términos de resolución para el mercado de dispositivos móviles está en Nigeria.

Tienen un tribunal que se aboca a la industria de dispositivos móviles. Todos los actores del mercado de dispositivos móviles pueden plantear sus demandas, sus quejas allí, y la gente tiene una vía de acción allí. Y pueden ver en un par de meses qué es lo que sucedió y los resultados.

Ahora volvamos al negocio o mercado de los nombres de dominio. Yo soy registrador en Senegal. Cuando la gente tiene un problema no sabe a quién recurrir.

Las regulaciones en nuestro entorno, realmente, o lo entes reguladores no tienen idea acerca de lo qué es un negocio de internet, no aprenden al respecto, no tienen nuevas capacidades. Necesitan una capacitación para poder recurrir a la organización relevante con un problema así.

Yo tengo un problema de un delito cibernético quizás me lleve meses, años, incluso puedo tener un funcionario policial frente a mí y le va a llevar meses entender qué es lo que le estoy diciendo. Si es un problema de ccTLD quizá tenga suerte de que en última instancia lo dirija al ccTDL que no va a poder solucionar el problema, pero al menos lo puede escuchar y entender que es un caso de abuso.

Porque el tribunal en sí mismo, la ley en ese país no está diseñada para abordar el delito cibernético.

No había mecanismo o interfaz que el registrador o el usuario pueda utilizar.

Yo les sugeriría a la ICANN y a la organización que, necesitamos una manera estructurada de respaldar y hacer cumplir o reforzar a los países que tienen esta problemática. Algunas se relacionan con la ley, con las regulaciones que organizan al mercado y a los actores, y a todas estas instituciones que intervienen en el sector, si no solucionan esto, el (registratario) de África o del tercer mundo, no tendrá confianza en el sistema y no va a apostar a ese sistema. Entonces, en última instancia, no se sorprendan si ven una muy baja introducción de nombres de dominio en la región o en el país. Porque el usuario va a decir "¿qué pasa si tengo un problema con mi revendedor o mi integrador o el proveedor de servicios de "web hoster"?

Entonces quizás prefieran estar en una interacción cara a cara.

Nii Quaynor: Gracias. Supongo que parte de mi pregunta aquí ya fue expresada. Voy a hablar de las bajas que mencionó Titi, hay muchas preguntas que quisiera hacer.

Ahora se da de baja un sitio web y aun así y la dirección de IP sigue allí sin cambiar en nombre. Y lo mismo sucede cuando se habla de la baja de películas. Es exactamente lo mismo. Entonces ¿Por qué no se puede volver a la dirección de IP y simplemente borrarla del sitio?

Intérprete: El orador está hablando fuera de micrófono.

Bien. Por favor. Respóndame con nombres y plazos para que pueda entender. Yo no tengo conocimiento técnico y creo que toda la información y el (…) viene a África como si fuera un tsunami.

Y mucha gente ni siquiera se preocupa pero ¿Qué pueden hacer ustedes respecto de la legislación y de las leyes?

Creo que esa sería mi pregunta general. Gracias.

Rafidah Mat Isa: Hola. Soy Rafidah de la Comisión de Telecomunicaciones de malasia. Y tengo una pregunta para Rod.

Actualmente nuestra comisión trata temas de bloqueo, lamentablemente, pero estamos más concentrados en el bloqueo por suplantación de identidad. Porque no queremos que la gente sea defraudada por los sitios web. Y hasta el momento hemos tenido una muy buena regulación con muchos de nuestros proveedores de internet, como “yahoo”, “google”, cada vez que los contactamos, ellos sacan el sitio web en pocos minutos y esto está ya fuera de sistema dentro de pocos minutos.

El problema que a veces tenemos es que ciertos sitios web que no están alojados por estas compañías y muchas veces no tenemos ningún tipo de respuesta. Utilizamos otra forma que es bloquear el DNS.

La nueva herramienta es muy buena definitiva, voy a volver a mi país y probarla. Y quisiera saber cuán rápido o con qué velocidad se da la respuesta. Cuál es el tiempo de respuesta? Porque actualmente tenemos dos casos para bloquear el servicio –en el caso de phsihing o suplantación de identidad – pero quizás ustedes puedan hacer más rápido. Con lo cual vamos a probar esa herramienta.

Ultimo comentario.

Hamza Aboulfeth: Soy de Marruecos. Soy un registrador acreditado por ICANN y mi pregunta es una pregunta directa. Me gustaría saber, como compañía marroquí ¿Qué leyes deberíamos aplicar y seguir? ¿Son las leyes de Marruecos, las de Estados Unidos o las canadienses? Ya que también tenemos nuestros servidores localizados en Canadá.

Y como también los podemos tener en Francia o algún otro lugar.

Esto depende de nuestra ubicación? O en algún momento alguna persona, un oficial de Marruecos puede hacer cumplir la ley? O alguien puede venir y pedirnos que cumplamos con la ley o solicitarnos información para poder dar de baja a un sitio web.

Y también quiero hacerme eco de los comentarios de mi colega. Estar en África y hace que nuestros usuarios finales entiendan la idea de a quién contactar en caso de que tengan un problema.

Si ustedes compran un sitio web de alguien que desaparece de una día para el otro y no queda nada, no hay sitio web, no hay nombre de dominio. Bien entonces ¿A quién deberíamos recurrir para solucionar este problema una vez por todas?

Nii Quaynor: Muchas gracias. Al menos tenemos muy buenas preguntas. Y lo que vamos a hacer. Vamos a comenzar desde aquella punta para pedirle a los colegas que hagan un comentario final.

Y que quizás presenten nuevas preguntas o responden nuevas preguntas.

Titi!.

Titi Akinsamni: Ojalá pueda ser breve. Quiero decir fui al "web cast" de nuestra sesión y me di cuenta que hay un comentario y es público así que lo voy a leer.
Se indica que hay algunos clichés que aparecen y voy a responder con mi comentario final.
No podemos huir de los clichésI y de los temas repetitivos, en tanto y en cuanto no los tratemos. Un ejemplo típico, y es una de las preguntas que surgió aquí. ¿Por qué simplemente no se quita la dirección de IP?
¿Por qué? En tanto estos temas no se entiendan en su totalidad y no se traten totalmente y no nos aseguremos de que todos lo entiendan, no vamos a seguir avanzando.

Mi segundo comentario es el siguiente. En cuanto a las bajas del DNS hemos hecho avances, claro que sí, pero muchos tienen que ver con las propuestas que tenemos frente a nosotros. ¿Qué vamos a hacer? ¿Cuándo vamos a seguir avanzando más allá de las charlas, los paneles y las conferencias? ¿Y cuándo vamos a tomar acciones?
Se han presentado ideas, pero sea lo que tengamos que hacer hay que hacerlo dentro de los que es la mayor brevedad posible. No importa si son a nivel de gobierno o de los proveedores de internet. Gracias.

Don Blumenthal: Me gustaría dirigir los últimos comentarios a la sala. En primer lugar, en cuanto a las leyes que hay que considerar, es un campo que estamos desarrollando aún. Sigue funcionando. Si uno tiene servidores en Canadá, tiene que considerar las leyes de Canadá. Si tiene base en marruecos tendrá que ajustarse a las leyes de Marruecos. Esto está tratándose en diferentes niveles.
Con respecto a dar de baja a un número de IP, y no estamos hablando de un nombre de dominio, que es algo distinto. Una vez más, podemos o

supongo que podemos avanzar con el número de direcciones. Y creo que se ha dirigido o se ha dado un enfoque diferente y esto no es una solución mágica. Hay lugares que son remotos y necesitamos mecanismos especiales para llegar a estos.
Para referencia, quiero cerrar porque estamos terminando y tenemos un grupo de trabajo trabajando en este punto.

Rod Rasmussen: Bien. Quiero responder la última pregunta realizada. El Programa APWG tiene un programa de suspensión. Si las cosas se están haciendo dentro de las dos horas, ajústense a esto. El proyecto de suspensión de registros probablemente va a estar ejecutándose y este programa de suspensión quizás pueda bloquear parte del contenido de internet.

Nii Quaynor: Si no tienen comentarios entonces no hay que hacer comentarios.

Michael Moran: Bueno. Yo creo que tengo un comentario más y que tiene que ver con la capacidad de incrementar el cumplimiento de la ley. Quizás no responde directamente a la pregunta del orador de la audiencia, peo estamos haciendo muchos esfuerzos, trabajando mucho en esta área y necesitamos llegar a la mayor cantidad de países posibles. Así que por favor tengan en cuenta de que se están llevando a cabo estas actividades en un trabajo lento, y hemos hablado en las diferentes regiones y estamos haciendo esfuerzos. Gracias.

Lanre Ajayi: Nigeria sigue luchando contra el ciber delito porque tenemos varias razones para hacerlo. Primero porque admitimos que existen, en segundo lugar comenzamos a luchar y admitimos la colaboración internacional con la conformación de este panel. Y la colaboración

solamente no tiene que ver con la lucha del ciber delito, tiene que ver también con los temas de jurisdicción y solamente podemos luchar contra el delito cibernético si tenemos un enfoque de multi-jurisdicción y esto tenemos que hacerlo en forma colaborativa.

Y en tercer lugar, también hemos adoptado un compromiso de múltiples partes interesadas para una mayor apertura y para poder luchar contra la ciber delincuencia. Algunos de estos ciber delitos si, están disminuyendo en Nigeria. Gracias.

Pierre Dandjinou: Bueno. Brevemente creo que él hablo de la colaboración y lo que me gustaría decir es en cuanto al desarrollo de capacidades. En cuanto a África creemos que tenemos que continuar trabajando y específicamente hay países que necesitan sus estrategias propias de ciber seguridad y se está trabajando.

Quizás las mejores prácticas que necesitamos desarrollar son en África y Arica las está implementando. El ÁfricaCert es una de ellas.

Nii Quaynor: Gracias Creo que han hecho un gran trabajo hasta aquí. Ha sido una larga jornada. Creo que hemos terminado con las discusiones y me alegra haberla tenido.

Les agradezco a todos por su participación.

Final de la transcripción -