TERRI AGNEW: Buenos días, buenas tardes, buenas noches. Bienvenidos al programa de creación de capacidades de At-Large, a este seminario web en relación a la comprensión y distinción entre las ciberactividades, el día de hoy, 15 de abril de 2015, a las 21 UTC.

No vamos a pasar asistencia porque es un seminario web. No obstante, quiero recordarles a todos los participantes que silencien sus micrófonos y parlantes y que mencionen sus nombres, no sólo para la transcripción, sino también para que los intérpretes los identifiquen en el canal lingüístico correspondiente.

Contamos con interpretación en francés y español.

Ahora le cedo la palabra a nuestro moderador, Alan Greenberg.

ALAN GREENBERG: Muchas gracias. Quiero decir que Tijani Ben Jemaa no va a poder participar de la llamada de hoy, pero él también es parte de esto.

Me parece que hoy es un tópico bastante interesante y un tanto distinto de lo que solemos tratar, porque tiene que ver con no se relaciona con las actividades de la ICANN o con la esfera de la ICANN, sino que más bien un tópico general y parece bastante importante. Yo pude ojear las diapositivas de la presentación y, por supuesto, es una presentación interesante. Y ahora le voy a dar la palabra a Steve Conte, para que proceda con la presentación.

STEVE CONTE: Muchas gracias, Alan. En realidad, quiero decir que esta es una presentación preparada por Dave [inaudible]. Así que yo voy a darla, pero él la preparó. Y no quiero recibir crédito por esta presentación, que en realidad hizo mi colega Dave [inaudible].

Aquí tengo una lista de participantes y sé que hay algunos que conozco y otros que no conozco. Yo debo decir que comencé a trabajar en la ICANN en el 2002, cuando la ICANN era bastante pequeña, por cierto. Éramos muy pocas personas trabajando dentro de la ICANN. Y yo me desempeñé dentro del departamento de IT, y también me encargué de ciertas cuestiones relacionadas con la IANA, hasta que comencé en este lugar, donde me desempeño como jefe de seguridad. Y también trabajé con John Crane. Y también me complace ver que hay caras nuevas, y también me complace ver caras que ya conozco.

Yo soy un presentador muy abierto, y por lo tanto, si tienen algún comentario o alguna pregunta, lo pueden hacer. Pueden hacerlo durante la presentación, o bien al final. Pueden interrumpirme cuando lo deseen. En realidad, pueden hacerlo como quieran.

En primer lugar, vamos hablar sobre el entendimiento y la distinción entre las ciberactividades o actividades cibernéticas. Y tengo una presentación y les voy a contar un poco a qué se refiere con esto, y esto es en relación a la ICANN y al equipo de SSR, porque esto tiene que ver con ciertas actividades legales.

No voy a leer las diapositivas palabra por palabra, sino que quiero señalar aquí que la palabra "ciber" es un término muy amplio, que está muy relacionado con diferentes cuestiones. Es difícil poner un título, porque hay muchos periódicos, muchos medios, o redes sociales, que hablan de ciberataques o ciberactividades. En realidad, tenemos que determinar qué tipo de actividades cibernéticas se llevan a cabo, porque son diversas.

Lo que vamos a hacer es considerar lo siguiente: vamos a considerar 3 puntos diferentes. Vamos a hablar de los medios, los motivos y las oportunidades. Esto lo vamos a describir en las próximas diapositivas. Seguramente vamos a hablar de los medios financieros y también de los medios tecnológicos y los intelectuales. Luego, en cuanto a los motivos, tenemos varios: políticos, económicos, financieros. Y también, en cuanto a la oportunidad, tiene que ver con el acceso a Internet.

Ahora bien, si nos acercamos o consideramos más de cerca el tema de los medios, vamos a ver que hay varias actividades y no estamos hablando únicamente de actividades criminales en este punto. Hay muchas actividades también que son legítimas o empresas legítimas, que son atacadas mediante actividades ilegítimas. Muchas de estas actividades necesitan ser financiadas. Luego tenemos la financiación por parte de los gobiernos, las ONG, o las comerciales, que realizan actividades cibernéticas para poder, por ejemplo, ofrecer fuentes abiertas o algunos beneficios digitales.

En cuanto a la financiación criminal, aquí tenemos que tener en cuenta la cantidad de correos electrónicos que se envían, que hay

ciertas actividades criminales o delictivas que tratan de obtener la información de su tarjeta de crédito, o tratar de *hackear* la computadora, para poder obtener los datos del usuario desea computadora, y sus credenciales, a fines de realizar ciertas actividades.

Luego tenemos las actividades que tienen que ver con el activismo y hay una palabra que es el *hacktivismo*, que es una palabra que se utiliza para describir una organización, o un grupo de personas, que se encargan de *hackear* con fines delictivos.

En cuanto a la oportunidad, la Internet es un acceso abierto de infraestructura tecnológica común y este poder deriva de la adaptabilidad. Esta actividad es fabulosa, porque, de alguna manera, representa el modelo orgánico que es Internet, es decir, cómo funciona la Internet, hoy por hoy.

Hace 20 años nosotros teníamos una estructura muy diferente y posiblemente el protocolo HTTP era distinto. Entonces, conforme crecen las facilidades, crecen las actividades, y esto requiere ciertas organizaciones, como el IETF, como la UIT. Es decir, diferentes organizaciones que se focalizan en las necesidades de los usuarios y las abordan. En este caso, también tenemos actividades legítimas y actividades que no lo son.

En cuanto a los motivos, tenemos diferentes objetivos. Hay objetivos políticos, objetivos comerciales. Tenemos también objetivos comerciales u otro tipo de objetivos.

Y en cuanto a los objetivos por ejemplo políticos, seguramente haya correos electrónicos, por ejemplo, que promueven cierto tipo de información política o cierto tipo de discursos, o cierto tipo de agenda, que tienen que ver con este tema puntual.

Y lo mismo sucede con el área comercial. Aquí, en cuanto a lo comercial, también se puede tener ciertas cuestiones con el buscador, donde se puede obligar al consumidor final a visitar ciertos sitios web o usar ciertos buscadores que pueden obtener cierta información de lo que hace o navega el consumidor. Entonces, los proveedores muchas veces utilizan esto para tener una mejor idea de qué ofrecer a los consumidores.

Cuando hablamos de las actividades cibernéticas, también tenemos ciertos escenarios, en particular, a tener en cuenta. Uno de ellos es la ciberseguridad. En este caso, hablamos de que no hay una definición exacta de lo que es la ciberseguridad porque es difícil definirla. Finalmente se habla de una serie de prácticas y la ICANN, mediante su equipo del SSAC, realiza cierto tipo de actividades de ciberseguridad. Aquí hablamos entonces de una serie de prácticas y medidas para proteger a las redes y a las computadoras y también tenemos que tener en cuenta a los dispositivos móviles, que navegan en Internet actualmente. En este caso, no hablamos necesariamente de una computadora de escritorio o de una notebook, sino que también hablamos de dispositivos móviles. Y los datos que esto implica, están sujetos a ataques.

Y estos ataques pueden tener distintas formas. Pueden ser un ataque de *phishing*, o suplantación de identidad, puede ser ataques mediante correos electrónicos, puede ser un ataque mediante una computadora que en primer lugar no estaba funcionando y luego se puede acceder a través de la computadora a otra, es decir, todas estas cuestiones tienen que ver con actividades cibernéticas y la ciberseguridad.

Ahora bien, ¿qué es un ciberataque? Es un ataque en línea, que puede ser un ataque digital o físico y por lo general, estos están dirigidos a activos digitales. Hace algunos años, recordarán que hubo un ataque a Microsoft y en ese ataque se utilizaron los servidores raíz para propagar el ataque. Entonces, se mandaban, a través de estos servidores raíz, mediante el ataque, diferentes paquetes en representación de Microsoft y parecía que no nos estaban atacando. Y de esta manera se lleva a cabo un ataque.

Esto, en realidad, es una forma de ataque dentro de Internet, pero también existen otras metodologías para atacar que tienen que ver con los activos físicos. Por ejemplo los que se realizan en los cajeros automáticos.

Luego tenemos el ciberdelito. Esta es una actividad online que ha sido clasificada como delito, o es una actividad online que se comete, o se lleva a cabo, en contra de o violando una determinada ley. Aquí trabajamos con las agencias de cumplimiento de la ley, con organizaciones de todo el mundo. Y lo que hacen es tratar de buscar criterios para poder frenar esto.

Hay muchas actividades que tienen un componente de ciberdelito. Como por ejemplo, enviar un SMS, o un correo electrónico con cierta información, o con ciertos fines, cuya finalidad es tratar de robar la identidad del usuario para poder utilizarlo en Internet o en diferentes redes.

Luego tenemos la ciberguerra. Estos son ataques a nivel de un Estado Nación, mediante o por otro Estado Nación. Esto se lleva a cabo entre naciones. No tengo información muy detallada al respecto, pero hay individuos en cada lugar del mundo, no solamente los Estados Unidos, que trabajan mayormente en la mitigación de estas actividades. Y este es un punto muy interesante, porque aquí hay que determinar si el ataque proviene de una delegación militar, con un objetivo puntual, o si esto es un ataque real, o no, que proviene de un individuo. O si proviene de un organismo o un grupo no gubernamental, o de un gobierno. Así que generalmente es muy difícil determinar cuál es la fuente del ataque, es decir, de dónde proviene el ataque. Y, dependiendo del tipo de ataque, un gobierno puede determinar qué medidas tomar. En algunas ocasiones, pueden utilizar ciertas medidas y, para producir un ataque a un gobierno legítimo.

Luego tenemos el ciberterrorismo. En este caso, esto es un ataque e intimidación mediado en forma digital a un ciudadano, a la ciudadanía, o a los civiles de una nación para personalizar la guerra. Básicamente, esto tiene que ver con un ataque de un civil a otro civil, o de un grupo civil, o de una empresa a otra, pero no necesariamente va dirigido a un gobierno. En realidad, es una actividad delictiva y básicamente, o

mayormente, esto proviene de un grupo de ciudadanos que ataca a otro grupo de ciudadanos con fines de guerra.

Luego tenemos la cibervigilancia. Esto es en realidad el recabado y monitoreo de información mediante formas digitales y esto puede ser un ejemplo. Por ejemplo, ustedes abren sus buscadores y pueden buscar diferentes productos, sugerencias, o también puede suceder a nivel de gobiernos, cuando los gobiernos monitorean ciertos servidores, o buscan palabras clave y esto puedo hacerlo yo con mi hijo, para asegurarme que mi hijo no visite ciertos sitios web en la red.

Esto engloba una serie de actividades. Esas son las actividades de ciberseguridad y en realidad, hay que darles un contexto a la tarea recibe vigilancia para determinar cuál es el grupo de actividades que se realiza en relación a la seguridad y a la vigilancia.

Y luego tenemos al ciberactivismo y a las actividades de *hackeo* o de *hacker*. En realidad, estas son las entidades no comerciales o comerciales que protestan, o un grupo, o nación, o un individuo. Esto se puede dar en las redes sociales… Perdón, estoy salteando algunos conceptos. Luego voy a volver a hablar de estos conceptos. En realidad, se trata de un grupo de *hackers* o de entidades que quieren enviar un mensaje, por ejemplo porque alguien les ha hecho enojar, o porque están en contra de algo, o quieren hacer una declaración sobre algo. Y lo que van a hacer es *hackear* un sitio web con determinado software, y luego van a cambiar la información. Esto sucede mucho también con las redes sociales o con los medios. Muchas veces, si nos encontramos es una sala de chat, o se hacen comentarios, o se dejan comentarios en un

blog, alguien también puede tomar esos comentarios y actuar en contra de nosotros y forzarnos a ver de qué manera pueden afectarnos.

Cuando hablamos de actividades de *hacker*, en realidad estamos hablando de una organización que trata de enviar un mensaje, de una manera que no es legal. En este caso, hablamos de activismo. Esto se puede dar en la forma de un correo electrónico, pero quizás en parte de una actividad, o del activismo. Puede ser un mensaje por algo que molesta en general, o por enojo en general. Y es una forma de enviar el mensaje. En este caso, y a este nivel de activismo, no se habla de un ataque, el objetivo no es atacar sino brindar información o crear conciencia, o bien tratar de disuadir sobre una determinada cuestión. Y cuando hablamos de una empresa o entidad que hace activismo legal, raramente se transforma en una actividad ilegal o pasa a ser ilegal.

De la mano de esto, de este "*hacktivism*", tenemos también una especie de vandalismo. Y hay quienes quieren *hackear* un sitio porque están en desacuerdo con la organización y a veces esto sucede simplemente porque los *hacker* quieren ser conocidos, quieren mostrarle al resto del mundo, especialmente a sus pares, que son *hacker*, que ellos pueden hacer este tipo de actividades.

En California, por ejemplo, tenemos mucho vandalismo, mucho graffiti en la ciudad, en las paredes, etcétera. Y de alguna manera esta es una versión digital de este tipo de vandalismo. Hay distintas definiciones de quienes son estos chicos malos, y hay quienes hacen una marca, entonces la gente sabe que esa marca quedó allí, y pueden

enorgullecerse de esa marca. Dentro de sus círculos, los *hackers*, o cibercriminales, son muy conocidos.

Creo que lo mencioné antes, pero la mayoría de las actividades son exclusivamente cibernéticas en muy pocas ocasiones. Es decir que no son solamente actividades criminales, sino que son actividades físicas también. La mayoría de las actividades, si miramos el activismo como ejemplo, pocas veces tenemos una actividad cibernética únicamente. En general, se utiliza en conjunto con lo que están haciendo otras organizaciones, que tratan de utilizar eso como otro canal de llegar a la gente.

Cuando hablamos de las actividades criminales, casi siempre hay un componente físico en esa actividad criminal. También ellos quieren ganar algo, o lograr algo, o proteger cierta identidad, y quizás utilizan Internet como una forma de obtener la identidad y en algún punto esto también se utiliza en el mundo físico, es decir que hay, por ejemplo, una empresa que quiere tomar prestado 3000 millones de dólares, va a haber quien quiera recibir un poco de todo eso.

Cuando miramos entonces las actividades, queremos conservar de algún modo estas tres cuestiones que mencionamos: los medios, los motivos y la oportunidad. Y también tenemos queremos tratar de determinar si es que se trata de actividades criminales, si son actividades relacionadas con el activismo, o hay *spam*, cuándo *spam* en el correo electrónico que tenemos es criminal. Puede ser una parte importante. Y a veces es simplemente correo no deseado. Cuál es el motivo de todo esto. Cómo podemos cambiar de banco para poder

apoyar a Greenpeace. Hay muchas formas de que la gente puede hacer este tipo de cuestiones. Todos estamos tocados por la ciberactividad todos los días y debemos entender qué es este ataque de ciberseguridad para poder dar una respuesta. Una respuesta puede ser simplemente apretar el botón suprimir y borrar el correo. Y a veces la máquina puede estar comprometida, o si la identidad fue robada, todas estas son cuestiones que tenemos que tener en cuenta, para determinar qué sucedió y cómo se lo podemos describir a un organismo de aplicación de la ley o a una organización y podemos darle una descripción más detallada de qué es lo que sucedió, qué es lo que creemos que sucedió y por qué. Lo que pueda llevarlos a que tengan algo un poco más cercano a su búsqueda y a la mediación.

Antes de hablar de las preguntas, quisiera pasar a otro tema. Y no tengo diapositivas de esto. En la ICANN, nosotros hablamos de los nombres de dominio, hablamos de las direcciones IP, hay organismos de aplicación de la ley, organismos gubernamentales que trabajan específicamente con las actividades criminales. Entonces, ¿por qué esto es importante para la ICANN? El equipo de SSR, de seguridad, estabilidad y flexibilidad, es un equipo donde solamente cuatro personas, cinco personas y media, en realidad, son las que hacemos muchas cosas, que incluyen la capacitación, y una de las cosas en las que trabajamos cada vez más es la aplicación de la ley, para poder ayudarles a esos organismos que aplican la ley a entender el aspecto digital en el que pueden estar trabajando. Entonces, cuando hablamos sobre la cuestión de que las actividades cibernéticas o que las actividades no son específicas de lo ciber, estamos hablando específicamente del campo de los identificadores unívocos, estamos trabajando en tratar de ayudar a las

comunidades de la seguridad, y las de la aplicación de la ley, a que puedan entender no solamente el WHOIS, que es una parte importante, sino también en el DNS en general, como sistema, y cómo podemos empezar a utilizar el DNS, cómo los malos están utilizando el DNS y la comunidad puede utilizarlo cuando van a argüir un caso ante un juez. Y decimos "tenemos que dar de baja este sitio porque ellos están haciendo la actividad ilegal X y Z", pero ahora hay como una marca. Es decir, puede haber una marca antes de que podamos hacer otra cosa, o tomar alguna acción legal. Nosotros los asistimos a entender dónde quedan estas marcas, donde están estas huellas digitales que quedaron marcadas en Internet, para que ellos puedan en generar un caso, construir un caso, y tomar medidas.

A veces, en algunos casos, dado el aspecto "*no border*" de lo que es Internet, nosotros ayudamos también a coordinar estas actividades. Es decir, hay un centro de comando y control para un *botnet*, y en ese caso nosotros determinamos que estos dominios malos están todos registrados dentro de un registrador. También trabajamos con las dos organizaciones de aplicación de la ley y los registradores, para coordinar esa baja de ese sitio, porque, desde la perspectiva de estos malos, cuando nosotros vemos qué es lo que está sucediendo, vamos a cambiar inmediatamente la forma en la que operamos. Entonces tenemos que garantizar que todas las piezas estén en su lugar, que todos los procesos se sigan, y que el registrador, o el registro, porque algunas veces no sabemos muy bien a dónde vamos, pueda ver todos esos dominios al mismo tiempo.

Nosotros no estamos involucrados en ninguna de estas actividades, sino que somos un coordinador entre las dos entidades. Hacemos mucho de todo esto y hemos estado trabajando mucho con la aplicación de la ley durante el último año y medio a tres años, para poder determinar cómo utilizar el DNS, para encontrar el abuso y el uso indebido, y ayudarlos a plantear un caso.

Voy a parar entonces acá, voy a iniciar las preguntas, si alguno la tiene.

¿Hay alguna pregunta o comentario con respecto a esto?

ALAN GREENBERG: ¿Hay alguien que tenga una pregunta? Tenemos a Alberto, que va hablar en español.

ALBERTO SOTO: Perdón por la voz, pero estoy por un poco ronco.

Es muy interesante todo lo que acabo de escuchar y en LACRALO tenemos un plan de capacitación interno, que va a incluir temas de seguridad y ahora voy a incluir algo específicamente de ciberseguridad tomando esta presentación como base. Pero también entiendo que tendríamos que hacer quizás un poco más de actividad, no solamente hacia nuestros usuarios individuales de Internet, que es el objetivo nuestro, tratar de llegar a ellos, sino también a otras partes del modelo de múltiples partes interesadas porque en cada evento, en cada seminario web que hemos hecho, siempre hemos tenido la presencia de

gobiernos y proveedores de derechos de Internet, sociedad civil, comunidad educativa, etcétera.

Pero creo que, como LACRALO, solos, no vamos a poder, y me gustaría contar con algún tipo de participación, como para que hagamos algo en conjunto para que se explique qué está haciendo ICANN, y qué podemos hacer nosotros para llegar a un más amplio espectro del modelo de múltiples partes interesadas. Gracias.

ALAN GREENBERG: Gracias, Alberto.

Steve, ¿quisiera recibir varias preguntas y después tratar de responderlas todas, o ir una por una?

STEVE CONTE: Como quiera.

ALAN GREENBERG: Ya que tenemos la mano levantada de Holly, vamos a Holly y después volvemos a Steve.

HOLLY RAICHE: Gracias, Steve. ¿Tienen ustedes relación cercana con el GAC y las diferentes Unidades Constitutivas, la ccNSO, etcétera?

Porque la imagen que usted plantea, especialmente sobre las actividades que tienen que ver con los organismos de aplicación de la

ley y lograr que los gobiernos entiendan lo que ustedes hacen, y coordinar con ellos, parece ser un ABC de cómo enfrentar el ciberdelito. A mí no me gusta llamarlo así, pero así lo llamamos, y también del ciberterrorismo. Y esto puede incluir a distintas actividades que están relacionadas con la ICANN.

STEVE CONTE: Gracias Holly y Alberto. Voy a poder responder a ambas preguntas, con una respuesta parecida. Y si no respondo, por favor pidan aclaración.

El equipo de SSR trabaja muy de cerca con el grupo de partes interesadas globales, porque ellos tienen sus pies sobre la tierra y son ellos quienes tienen las comisiones, la relación con los gobiernos y con las organizaciones en esta región, así que quisiéramos trabajar dentro de la ICANN con el GSE, para poder llegar a otros.

Holly, sus preguntas son muy importantes, y una de las cosas que va hacer el SSR es aumentar nuestra relación con las distintas organizaciones, partes interesadas y consejos asesores dentro de la ICANN.

Este es uno de los modelos, pero nosotros hemos hablado frente a la ccNSO, creo que fue en Londres, donde hablamos casi a nivel de uno a uno con los miembros de la comunidad de la ICANN, pero estamos tratando de llegar a otros y hacer que nuestras relaciones se han más fuertes.

Como parte de esto, esto es algo que va a aparecer en el final de la presentación, yo tengo un pedido para el grupo de ustedes. Porque yo,

creo que fue en la reunión de Los Angeles, tuve una relación con él ALAC y lo que nosotros quisiéramos es ver cómo podemos coordinar actividades y tener esa participación del comité asesor At-Large, especialmente en el aspecto de la estabilidad y seguridad del modelo de la ICANN.

Una de las cosas que estamos haciendo, es que estamos empezando una capacitación sobre seguridad, estamos construyéndola de a poco, porque somos un equipo muy pequeño y todos estamos viajando bastante seguido. Pero lo que tratamos de hacer es estar a nivel del consumidor con distintas actividades, a nivel gubernamental también, y ver cómo ustedes, como personas o como organización, pueden ayudar al sistema, de algún modo. Y así poder estar seguros de que mi hijo no esté haciendo clic en correos electrónicos que son de *phishing*. Es decir que podemos tener así una conversación un poco más inteligente con las distintas entidades. Lo estamos haciendo con el entrenamiento que estamos generando, lo estamos haciendo también probablemente con una serie de actividades de aprendizaje online, donde ahora estamos generando un modelo de [DLP], para aprender en ICANN, para que nosotros podamos entender este módulo de DNS, que cualquiera va a poder ver.

Entender el DNS, va a ser un curso y vamos a hablar realmente sobre las bases, los fundamentos de lo que es el DNS. Vamos también, una vez que esto esté completo, a solicitar los aportes de todos los grupos y queremos estar seguros de que no los construimos para nosotros sino para gente como ustedes. Y queremos estar seguros precisamente de

que vamos estar al nivel adecuado, utilizando las piezas adecuadas y que nuestra audiencia esté recibiendo información valiosa.

Otra cosa que estamos haciendo también, es recolectar distintos recursos sobre la seguridad, y mi pedido al ALAC inmediato es que miren esto que acabo de colocar, para ver si es que existe alguna diapositiva que falte en esa página, por favor dígannoslo. Si es así, lo vamos a incluir en esa lista. Se lo damos a aplicación de la ley, a la seguridad pública, porque queremos empezar desde abajo.

¿Eso responde a las preguntas de Holly y de Alberto?

HOLLY RAICHE: Para mí, sí responde a mi pregunta. Me estaba refiriendo a algunas de las actividades que están ocurriendo en Australia. Nosotros acabamos de designar una persona para ciberseguridad y ese tipo de cosas donde la seguridad y la sociedad de Internet están coordinando, porque hay mucha información que debe ser difundida y que seguramente sería muy útil tener un acceso a ese enlace, y ver qué es lo que tenemos ahí, como forma de utilizar al ALAC, precisamente para difundir la información a la que debemos obtener acceso.

STEVE CONTE: Estoy de acuerdo con todo eso. Por favor, como les dije, hagan clic en este enlace y vean toda la información que tienen allí.

HOLLY RAICHE: Bien, muchas gracias, Steve.

ALAN GREENBERG: ¿Hay alguna pregunta o comentario con respecto a esto?

Yo di mi primera presentación sobre *spam* y creo que, allá por el 2002, así que voy a ver si puedo recabar esta información, porque fue muy interesante. Y también hubo una presentación sobre el ciberdelito, 15 años antes.

¿Qué es lo que ve usted en cuanto a los cambios? Claramente tenemos altas y bajas, tenemos problemas, pero, ¿cuáles son las tendencias generales que usted ve?

STEVE CONTE: Es una pregunta interesante, Alan. Desde mi propia perspectiva, y en realidad yo no soy de una parte de cumplimiento de la ley, sino que lo veo como lo ve la comunidad, en los últimos 10 años se han incrementado varias actividades, pero también hay un incremento de los usuarios en Internet. Entonces, cada vez más, vemos actividad que tiene que ver con el *phishing*, con la recaudación de información, cada vez hay más grupos de cumplimiento de la ley tratando de abordar estas actividades y de frenar estas actividades, como por ejemplo el *phishing*.

Por ejemplo, la FDA en Londres trabaja con esto, y al diferentes organizaciones que trabajan con estos temas, porque están muy preocupadas con la cuestión farmacéutica dentro de Internet. Y esto es

algo real, no es algo que afecte solamente a una persona, sino que pone vidas en peligro. Hay muchos otros aspectos que van surgiendo dentro de la actividad cibernética. Hay actividad delictiva y hay comunidades que abordan estas cuestiones. Pero el *phishing* parece ser la actividad más repetitiva a lo largo de todos estos años.

ALAN GREENBERG: Muchas gracias. Por favor, quiero pedirles a todos que silencien sus micrófonos, porque escuchamos mucho ruido de fondo. Por favor, recuerden silenciar los micrófonos cuando no están hablando.

Adelante, Alberto, y luego le damos la palabra a Holly.

ALBERTO SOTO: Sí la nueva, nosotros estamos haciendo, con nuestras organizaciones, un informe individual de distintos países, ciertas llegadas a los usuarios individuales, donde estamos hablando de *phishing*, de trata de blancas, de pornografía infantil, etc., y tenemos llegada a los usuarios individuales. En nuestro último seminario web estuvo dado como tema el GAC y el usuario individual, y hemos quedado con la vicepresidente del GAC en tratar de acercar más, e inclusive participar de reuniones, tanto de ellos, como las nuestras, para poder tener una mejor relación.

Particularmente, eso nos tiene que servir porque en muchos países de Latinoamérica, no hay ninguna ley respecto de estos temas. Hay muy pocos, y hay muy pocos equipos técnicos con la capacidad necesaria y equipamiento, porque es bastante oneroso.

Entonces, la tarea nuestra está orientada también a tratar de generar, de abajo hacia arriba, tal cual el sistema de la ICANN, la generación de las políticas necesarias, de las leyes necesarias en cada país. Un ejemplo muy claro es que, por más que alguien tenga un equipo, no hay obligación de retener datos de tráfico, por ejemplo en Argentina. Es decir que un proveedor de servicios de Internet al cual un juez le ordene, por un delito, la investigación de un delito, que le de la actividad de una dirección de IP, al año que sucedió, es altamente probable que no pueda conseguir nada, porque no hay obligación de retener esos datos de tráfico. Realmente, estamos ante un problema muy complejo nosotros y estamos tratando de encarar todo esto. Gracias.

ALAN GREENBERG: Gracias, Alberto.

Steve, ¿tiene algún comentario?

STEVE CONTE: Sí, Alan. El comentario de Alberto es sumamente interesante. En junio vamos a estar en Buenos Aires y voy a preguntarle a la gente cuántos tienen el mismo problema, y seguramente la mayoría va a levantar la mano. Entonces, esto es un tema muy importante. No es una consideración única, pero sí es muy importante.

Usted mencionó la falta de equipos y políticas. En los últimos tiempos, lo que sucede es que hay dos grupos específicos que tienen que ver con el desarrollo de tecnología y de políticas, diría que hace unos cinco

años, en realidad, y ellos trabajan continuamente para poder reunir a estos dos grupos, para que trabajen y para que también participar a los diferentes individuos dentro de estos temas. Y me parece que esto de lo que estamos esperando, porque las políticas de Internet no pueden funcionar sin la tecnología y la tecnología no se puede construir tampoco si no tenemos políticas.

A ver, la Internet ya más lo que solía ser, y voy a decir, entre comillas, que se está cada vez más integrando y tiene muchas cuestiones positivas, y cuanto más podamos avanzar, mejor va a ser, pero cuanto más podamos avanzar en las regiones, mejor va a ser también para estas regiones, si les ayudamos a mitigar este tipo de actividades, a través del desarrollo de políticas y si los individuos participan, teniendo por ejemplo aplicaciones o protocolos más funcionales, o políticas. Creo que todo esto va a contribuir.

ALAN GREENBERG: Muchas gracias, Steve.

Adelante, Holly.

HOLLY RAICHE: En realidad, ésta es una pregunta difícil. ¿Cuáles son los desafíos que presentan los nuevos gTLD y los IDN, en toda esta cuestión?

STEVE CONTE: Es una pregunta muy interesante. Esto es algo que abordamos dentro del equipo del SSAC. No hablamos únicamente de los IDN, sino también de la nueva ronda de los TLD que se va a llevar a cabo. Aquí tenemos que tener en cuenta qué tipo de actividades se llevan a cabo. Hemos hecho mucha investigación para determinar si los registradores hacen oídos sordos a las actividades de los usuarios y qué tipo de actividades son las más comunes, en cuanto a los nombres de dominio delictivos. Entonces, conforme surjan nuevos gTLD, tenemos que ver qué parte de esa registración difiere de la actividad normal. No tengo frente a mí las cifras concretas, pero si quieren las puedo buscar para decirles o darles resultados. Quizás esto los pueda ayudar de alguna manera a mitigar estas actividades.

HOLLY RAICHE: Muchas gracias. Seguramente vamos a comenzarlo al respecto.

KEITH DAVIDSON: Seguramente que sí.

ALAN GREENBERG: ¿Hay algún otro comentario o alguna otra pregunta que quieran hacer? Todavía nos queda tiempo.

Y Steve, creo que usted ha contestado todo lo que posiblemente se le podría haber preguntado.

¿Algún comentario de cierre, un comentario final?

STEVE CONTE: Simplemente quiero decirles que, cuando estuve en la reunión de Los Angeles, en la reunión de la ICANN que se celebra Los Angeles, en el ALAC, realmente, me abrió mucho los ojos. Fue muy útil. Y no sé si el SSR ha hablado directamente con el ALAC. Esto seguramente lo vamos a hablar con John Crane, para poder estar presentes en las reuniones del ALAC. Y esto espero que no se vea como una necesidad de interrumpirlos, o de infringir en sus actividades, simplemente de lo que la comunidad de ustedes habla, y espero que podamos estrechar nuestras relaciones. Así que ésta es una gran oportunidad. Yo quiero agradecerles a todos por darme la oportunidad de interactuar con ustedes y de tener este diálogo.

ALAN GREENBERG: Muchas gracias. Una serie de comentarios. Hay una mano que está levantada, pero también hay otra pregunta de Olivier, que dice si esta reunión, esta llamada, no tenía 90 minutos asignados. En realidad, sí, pero mucho de lo que hacemos, tiene que ver con los usuarios, se focaliza en los usuarios. Y mucho de lo que hablamos tiene que ver con las formas, de no necesariamente cómo se puede ver afectado del usuario final, sino más bien de cómo se puede hacer que la experiencia sea mejor, o más segura, o más estable. Esto es de lo que hablamos, en su mayoría. Y aquí estamos hablando también de las cuestiones del SSR, que no todas caen dentro del control de la ICANN, pero que sí nos afectan. Con gusto, agradecemos cualquier participación.

Adelante, Olivier.

OLIVIER CRÉPIN - LEBLOND: Steve, muchas gracias por la presentación. Es sumamente interesante. A mí siempre me interesa la cuestión de los ataques cibernéticos y el ciberactivismo porque hay mucha actividad. Y la ICANN siempre está sujeta a estas cuestiones o al *spear phishing*, y este tipo de ataques. Este tipo de ataques dentro de la ICANN, ¿sería un ataque cibernético o estaría clasificado dentro de alguna otra cuestión?

STEVE CONTE: En la palabra *phishing*, es una actividad que tiene que ver con el de reemplazo de información. Si uno recibe un correo electrónico de alguien y uno ingresa a ese correo electrónico, puede ser de alguna manera pescado y se le puede robar información. Porque recibe ese correo electrónico de alguien que dice ser alguien que no es. Esto puede ser hecho únicamente por una persona, o una combinación. Ahora bien, muchas veces sucede que un individuo, o un grupo de individuos dentro de la organización quieren comprometer una organización, o a la red de la organización.

El SSR está involucrado con la seguridad, pero no les puedo decir exactamente de qué manera. Sí tenemos un ataque de *phishing* general y también tenemos ataques de *spear phishing*, dentro de la organización. Hasta donde yo sé, no sabemos puntualmente quién fue el culpable o el responsable, quién tuvo la intención de hacer esto, y cuáles son los motivos. Todavía la ICANN se encuentra trabajando con el correspondiente departamento, pero también con la agencia de cumplimiento de la ley, para poder determinar cuáles son los motivos

para este tipo de ataques. Todavía estamos tratando de construir todo esto. A veces es mucho más difícil de lo que parece determinar quién lo hace y por qué. Porque Internet tiene muchas actividades. Hay mucha actividad dentro de Internet y es difícil determinar los motivos.

Básicamente, cuando se ingresa en una mediación, cuando uno sabe que está siendo atacado, o se está comprometido, hay que actuar. Y la ICANN lo ha hecho de forma inmediata. Se tomó acción en cuestión de horas. Y esto le sucede a una organización que no necesariamente tiene que ser la ICANN. Tenemos diferentes procesos implementados para poder asegurar la red. Y también tenemos procesos, otro tipo de procesos, dentro de Internet, para poder recabar información y aprender de todo esto. Entonces, recabamos esa información y luego trabajamos con las agencias de cumplimiento de la ley para poder determinar quién lo hizo y qué se puede hacer y tomar acción al respecto.

ALAN GREENBERG: Muchas gracias. Quizás sea gracioso para algunos, pero mi primera experiencia con lo que llamamos *spear phishing*, o *phishing*, me pasó, si no recuerdo mal, hace unos cuantos años, allá por 1978, pero bueno, no tenía mucho que ver con lo que sucede ahora.

¿Hay alguna pregunta o comentario con respecto a esto?

Dev Anand está tipeando algo. ¿Quiere agregar algo?

Steve seguramente va a tener alguna otra oportunidad para hablar con nosotros. No tiene que repetir todo ahora.

¿Hay alguna pregunta o comentario con respecto a esto?

Dev Anand tiene un comentario y pregunta si habrá una presentación similar a la que se hizo anteriormente en Argentina. Sé que hay una presentación sobre un taller sobre seguridad pública.

STEVE CONTE: El taller sobre seguridad pública se va a llevar a cabo. Es un trabajo de la comunidad de la ICANN, junto con las agencias de cumplimiento de la ley, y seguramente sí se realice. Por lo general, hay sesiones abiertas y cerradas. Yo no sé qué están planificando ahora, pero nos han pedido ayuda.

En cuanto a las actividades y eventos del SSR en Buenos Aires, no estoy seguro, voy a trabajar con John Crane para determinar qué idea hay para Buenos Aires. Y no sé si se los puedo hacer llegar a través de Terri.

ALAN GREENBERG: Supongo que en realidad debería ser a través de Gisela.

STEVE CONTE: Entonces voy a hablar con el equipo del SSR para ver qué información tienen al respecto, y se los voy hacer llegar al ALAC.

ALAN GREENBERG: ¿Hay algún otro comentario?

Si no, muchas gracias, Steve, por su tiempo. Desde mi perspectiva, ha sido muy interesante y divertido. Le agradezco por esto.

STEVE CONTE: Muchas gracias a ustedes y voy a estar en Buenos Aires toda la semana, así que me pueden contactar.

ALAN GREENBERG: Voy a tratar de recordarlo. Y muchas gracias por contribuir con este tema.

STEVE CONTE: Para mí ha sido un placer.

ALAN GREENBERG: Nuevamente, gracias. Hasta luego. Gracias a todos por participar.

[FIN DE LA TRANSCRIPCIÓN]