Damas y caballeros, estamos por dar comienzo a nuestra siguiente sesión. Me gustaría presentar al señor Steve Crocker, ice Presidente de la Junta de Directorio de ICANN.

Steve Crocker: Gracias. Es un placer estar aquí con ustedes, la ceremonia inaugural y los discursos de las asignaciones de direcciones son actos difíciles de seguir así que, espero que haya asistentes a este Foro porque se ha hecho un gran trabajo. Hay un grupo de panelistas aquí con nosotros que van a hablar del abuso de DNS. Voy a intentar minimizar y maximizar de alguna manera el tiempo que tenemos.

En la pantalla ven el nombre de las personas que tenemos aquí presentes que son el señor Boscovich de Microsoft, a quienes le decimos Joe, de internet , Michael Moran de Interpol, Robert Flaim de la FBi, Glenn Watson de la FDA, Terry Stumme de la Agencia de cumplimiento de drogas de los Estados Unidos: están aquí presentes así que con esto, creo que vamos a comenzar ahora, ya, y permítanme pedirles a todos ustedes por la cortesía y por todos los que tenemos aquí presentes que se ajusten al tiempo que se les asignó, yo sé que va a ser algo difícil, pero bueno, les pido que traten de hacerlo y ojalá podamos logarlos. Así que señor Bosco le damos la palabra.

Richard Boscovich: Bueno. En primer lugar gracias por invitarme. Es un honor para mí estar aquí presente, y voy a tratar de hacer lo mejor posible y hablar lo mejor posible. Trabajo en Microsoft específicamente en un grupo de crímenes cibernéticos y uno de nuestros objetivos en el departamento de la compañía es ver e investigar las amenazas que tenemos y generalmente lo hacemos, y tratar de solucionarlas, tratamos de abordar las agresivamente y tenemos una serie de desarrolladores e ingenieros que se encargan de buscar el software malicioso y durante mi tarea allí nos tuvimos que focalizar en los "botnets" y nos dimos cuenta que en los últimos años los "botnets" son muy malos para la infraestructura y que se han utilizado para muchas actividades ilegales de internet, como por ejemplo el correo electrónico basura, lo que es la actividad de "phishing" cualquier cosa en la que ustedes piensen.

La estructura que tienen es la estructura del "botnets" y la manera en que se diseminan es peligrosa. Hace un año aproximadamente, mi equipo estableció esto y decidimos hacer algo agresivo, una campaña agresiva con estos "botnets", algo que tuviera carácter legal y técnico y resolvimos algo que muchos de ustedes ya conocen, y no fue en este foro sino en el anterior, que fue una herramienta denominada "waledac" para poder solucionar este problema. Esto fue lanzado en octubre de 2007 y en esa resolución de esa época se nos dio acceso a 700 mil dominios y dominios para este "botnet" específico, ahora la operación afecto a muchísimas computadores y luego la resolución final hizo que todas la computadores vinieran a nosotros e indicaremos que direcciones IP habían afectado y tuvimos que buscar en todo el país y limpiar nuestras computadores en todo el país.

La primera operación que nosotros llamamos la operación Mars que es una respuesta activa de Microsoft para la seguridad hizo que aprendiéramos muchas lecciones particularmente en este tema que hoy vamos a discutir, para hacer una operación cívica en los Estados Unidos, hay que tener en cuenta muchas cosas, porque para poder llevar a cabo esto y solucionar el problema del "botnets", teníamos que quitar los "botnets" y de alguna forma parecía fácil y otras no y había que tener un proceso inicial.

El tema fue difícil de seguir con respecto a los procedimientos y también y notificar a todas las personas relacionadas con los dominios que eran utilizados para el CNC y darles una alerta y esto era un problema importante, entonces, lo que hicimos fue ofrecer una solución bajo un TRO que nos permitió avanzar y quitar esto de los individuos y luego hacer un seguimiento con una audiencia cuarenta días después siguiendo los procedimientos. Ahora lo que buscábamos en la situación en la cual en esencia pudiéramos ver cómo era la estructura de ICANN con respecto al DNS y esto para mí fue algo que lo tuve que hacer en Microsoft.

Por ejemplo cuando tomamos un proceso de un UDRP como ejemplo, y aunque en algunas situaciones este proceso es útil especialmente en las disputas comerciales, uno puede ver lo que sucede después de que

expiran los períodos de tiempo, generalmente hablando esto es aceptable, pero cuando uno tiene un nombre de dominio particular que está siendo utilizado para un propósito malo y el titular de este dominio o quien lo registra han movido este dominio y uno comienza a perder control, tiene que comenzar nuevamente de cero, con este proceso de resolución de disputa alterno. Y por lo tanto es una manera de avanzar de manera extraordinaria.

Entonces. En lugar de ir a los registrantes que sería algo simple, en este punto hemos hecho un análisis de que el dominio solo ha sido dado para determinados usos, entonces decidimos apuntar al registrador.

Desde mi perspectiva se dijo que estaba fuera de las jurisdicciones de los Estados Unidos y que el caso POSCO que es el caso el que estamos hablando, excedía y tomamos un paso adelante y fuimos al registro. Y parece que la mayoría y si no todos los dominios con".com" tenían un ángulo jurídico y por supuesto del Nom.Com es de VeriSign y está dentro de los Estados Unidos, así que la Corte nos permitió emitir una orden por pedido de VeriSign para poder avanzar y determinar de dónde venían las conexiones.

Ahora, ¿Cuáles era los objetivos que nosotros encontramos conforme avanzamos en el proceso? Vimos que todos los dominios en el caso (…) eran registros chinos y todos requerían información. Un punto en particular, que yo iba a hacer una lista de los nombres de dominios y los registradores y había muchos nombres chinos, obviamente, esto sería muy incómodo hacerlo y muchos serían erróneos porque cada uno era erróneo era algo falso.

El proceso de registración del proceso de dominio estaba lleno de errores y había fraude, ninguna información era exacta y la información única que era exacta eran dos direcciones de email y la única manera de identificar y saber que estas pertenecían a alguien fue cuando hicimos un proceso por email y alguien en dos de estas direcciones abrió el email y lo leyó, no lo respondió, pero sí lo leyó y sí habían entonces recibido información en estas direcciones, bueno, quizá muchas no hubieran llegado, así que básicamente si uno considera los problemas en cuanto a la registración de los dominios desde el punto de vista legal, si se pueden identificar quienes tienen esos dominios nos podemos evitar todos los procesos legales o iniciar una especie de proceso legal contra la compañía o quien esté enfrente.

Esto también implica un problema difícil porque implica mucho tiempo.- En este caso en particular tuvimos un proceso y que lo llevamos a la Convención de La Haya y que fue en China, y llevó meses afortunadamente, tuvimos asistencia rápidamente cuando nos dimos cuenta de que habían dominios que se habían perdido en nuestra solicitud, y muchas compañías y empresas cooperaron con nosotros. Les voy a mostrar algo de los temas y complejidades que implican el abuso al Sistema de nombres de dominios. Estamos en una situación en que hay quienes toman ventaja del proceso de registración del proceso de resolución de disputas porque saben que tiene la capacidad de cambiar si es que así se requieren, entonces, esta fue la primera operación. Actualmente estamos en el proceso de otra operación que por supuesto

en el futuro planificamos seguir avanzando. Lo que vemos es que hay diferentes tipos de abuso del Sistema de nombres de dominio.

Ahora vemos (..) y Software malicioso, no sólo los “botnets” sino que afectan no sólo a los nombres de dominios sino que afectar al algoritmo y a la codificación del nombre de dominio en sí mismo, en un caso en particular hubo un software malicioso que genera 15 o 16 nombres de dominio a diario, así que si por ejemplo si este virus en particular controla un determinado protocolo va a tener un control y va a modificar las direcciones de IP y luego va a cambiar a un modo secundario y sigue avanzando y utilizando el generador de nombres de dominios y obviamente esto dicta que en esta situación hay que saber qué dominios van a aparecer y cuáles son estos dominios. Pero considerando el ejemplo los dominios en muchos de estos software maliciosos o afectados por este software malicioso, son simplemente cadenas de caracteres alfa-numéricos. Y nos preguntamos entonces quién registra esto y para qué, si hay alguien que busca esto que se registra cuidadosamente para qué lo hacen. Y si alguien presta atención en cómo estos dominios se pagan y de donde se originan, es algo que hay que considerar. Algunos de los temas con los que nos topamos cuando hicimos nuestra operación b49 fueron temas que nos determinaron que si se cambian o hay cambios en la etapa de las resolución de disputas o en otra etapa como por ejemplo en la delegación, puede haber un período de 24 horas donde ICANN puede ver si el registrador responde o no o puede este punto determinar si la información del registro es correcta o no.

Entonces estos son algunos de los ítems que son cruciales para seguir avanzando en el proceso conforme la amenaza de los “botnets” aumenta y hay que estar mucho más conscientes de cómo el sistema de nombres de dominios se está utilizando por los delincuentes cibernéticos.

Steve Crocker: Gracias. Joe le ceso la palabra.

Joe St. Sauver: Gracias. Tenemos diapositivas también. Bueno desde mi punto de vista una de las preguntas más interesantes es ¿Dónde va el “spam”, o donde se meten, en la infraestructura y cómo afectan los recursos y la infraestructura de los nombres de dominios? ¿Cuáles son los registradores que son victimizados por estos individuos?

Y creemos que en muchos casos va a haber una cantidad de registradores limitados que son sujetos al abuso y podemos trabajar con ellos para ayudarlos a lidiar con esta violación de su política que actualmente sufren. Porque creo que en muchos casos estos registradores son víctimas y también reciben “spam”. Y en otros casos pueden ser que el registrador por cualquier razón no pueda tomar acción contra quienes utilizan sus servicios y en ese caso saber qué

registrador parece tener ese problema, nos permite avanzar y tomar acciones como por ejemplo contra el sistema de abuso en el email.

Este es un tema que traje a colación en marzo del 2000 y se focalizaron al respecto y voy a darles entonces una versión muy condensada del material que surgió de esa reunión en aquel momento en San Francisco en 2008-

Maawg es una organización con la que quizás ustedes no estén familiarizados pero que lucha contra el "spam" y tiene muchos miembros que son proveedores de servicios e internet y también tienen registradores que participan en la actividad de esta organización.

Una de las cosas que me gustaría asegurarme de mencionar, es que si ustedes quieren participar ya sea porque son un registrador o no también serán más que bienvenidos y voy a decir también que yo he trabajado con Maawg, como un Asesor técnico sénior en esta organización así que si van a tratar de determinar qué registrador ha sido abusado lo que hay que saber es cuáles son los dominios q2ue se muestras y los dominios que se muestran están rastreados por una serie de organizaciones y quizás el más conocido es el Surbl y para darles una idea del impacto de este sitio, si uno va a un mensaje de mail, esta lista de mail va a tener una serie de dominios que puede tener entre un décimo y 4 ½ puntos de cosas por ejemplo "spam" y demás.

Así que hay una situación en la que la comunidad sostiene que hubo un gran impacto. Lo siguiente que se necesita saber es mapear los nombres

de dominios para el registrador y esto es un proceso simple. Supongamos que vamos a utilizar herramientas que ya están disponibles, uno puede ir al WHOIS y ver quién es el registrador de determinado nombre de dominio, esto generalmente es así, pero hay algunas excepciones; algunos ccTLD no ofrecen esta posibilidad por ejemplo o en algunos casos están muy limitados. Puede haber otros factores que hace difícil obtener esta información también, hablamos de la manera que se pueda hacer más eficiente pero la idea es conseguir la información necesaria para poder realizar este mapeo.

Antes de seguir hay que hacer un chequeo de lo que estamos viendo y asegurarnos de que antes de seguir avanzando en los registradores hay que ver qué ccTLDs están enumerados en las listas, 4% de los dominios eran ".info" y es importante entender esto, porque el ".info" tiene una reputación interesante respecto a luchar contra el abuso y tenemos que responder de manera apropiada y rápidamente y esta es una cosa que surgió. ".si.com" también es otro dominio.

Estos dominios colectivamente representaban el 90% de los dominios en la lista y entonces había una concentración ahí, algunos dicen "bueno, vamos a ver o asegurar algunos dominios" cualquiera sea, quizás en el futuro pero ahora no se puede ver de esa manera. Entonces esta enumeración tenía datos y de acuerdo al volumen de email usábamos un dominio y quizás había otros dominios que no se usaban mucho. Había que seguir avanzando e identificarlos.

Cuando comenzamos a mirar a los registradores otra vez había algunas cosas interesantes para anotar y nuevamente Go-Daddy es un

registrador muy responsable, entonces lo primero que se me vino a la mente, es que probablemente había un hecho relacionado con el tamaño y quizás no tiene que ver con la pate del mercado que ocupa el registrador sino que también hay dominios que están enumerados para cuando uno hace el mapeo, entonces uno tiene que comprender que hay que hacer el mapeo de manera gentil, para que no haya un operativo en los servidores de WHOIS. Así que la situación fue que uno veía algunos dominios que se iban rápidamente y también había algunos registradores asociados con ccTLDs particulares. Pero el punto es que podíamos seguir avanzando y obtener esta información base para nuestro registro. Y voy a avanzar en mi presentación porque esto no los va a ayudar si están sentados allí.

Bueno entonces ¿Cómo podíamos hacer para adaptarnos al "market share" o a la porción de mercado del registrador? Sabíamos que Go-Daddy es amplio y no es justo entonces que avanzaran sin hacer o sin tomar ninguna medida. Y había muchos enfoques que tuvimos que considerar. Entonces, hubo una serie de situaciones a sincronizar, había que ver la cantidad total de dominios que eran indeseables y por lo menos 2/3 estaban enumerados y esto representaba una porcentaje aquí. Al mismo tiempo no creo que se debería avanzar y obtener un pase libre como por ejemplo el 1% número inaceptable, pero si ese 1% de miles de millones de nombres de dominios es abusable, entonces sigue representando un importante número para resolver y esto es mucho más relevante, es algo que parece pequeño pero es importante, por ejemplo el 0,5% seguramente sea una cifra interesante y Go-Daddy es

un ejemplo muy amplio pero quizás podemos tener 20 mil o 15 mil casos de dominios abusados. Otro ejemplo quizás sería de 3 mil dominios Tucous, no esperemos milagros, pero la idea es reducir estos números. Una de las cosas que quiero decir y asegurarme que entienda es que hay mucho aún por hacer, esto es simplemente un ejemplo de lo que se puede hacer, la escalación del sistema de nombres de dominios es algo que hemos hecho y que seguimos haciendo y que nos ayuda a resolver los problemas existentes.

Pero también sería maravilloso ver si podemos avanzar en la proporción de un mapeo en los nombres de dominios diariamente, no necesariamente revisar el WHOIS continuamente pero si podemos obtener la información diariamente sería mucho mejor. Y también es importante saber que algunos ccTLD simplemente no proporcionan información sobre su fuente en absoluto, entonces, en este aspecto se requiere más transparencia y es algo que tenemos que logar de alguna manera, para poder tener un objetivo claro en general.

Steve Crocker: Gracias Joe. Muchísimas gracias.

Michael Moran: de Interpol. Soy Michael Moran tendría que decir que aquí en Estados Unidos soy miembro de la policía irlandesa nacional y también trabajado para la Interpol, es una Organización Policial Internacional.

Rápidamente quiero presentarles a la Interpol como base para tratar de despegarnos de esta imagen hollybudense que hay de Interpol, no vamos a ver ningún tipo de helicóptero etc., etc. ni nadie que baje de un helicóptero. Nosotros trabajamos con comunicaciones, bases de datos, soportes operativos y transferencia de habilidades.

Nosotros aseguramos una red mundial que conecta a 188 países miembros y cada uno tiene una agencia central y cada agencia central en cada país ocupa un alto lugar en la jerarquía policial. Tenemos bases de datos, huellas dactiloscópicas, bases de NI, de ADNs, también bases de datos de vehículos robados y también una base de datos para explotación sexual infantil.

Como parte del respaldo operativo tenemos un subgrupo de crímenes organizados, de seguridad pública y de terrorismo y el tráfico de personas también dentro de esa sección, tenemos –

Bueno voy a darles un pantallazo general de dos operaciones relacionadas que se han dado en los últimos 4 años todas ellas basadas en la web y todas tienen que ver con el abuso de DNS.

Antes de comenzar quiero dejar bien en claro que no voy a utilizar palabras como pornografía infantil etc. Sino que voy a nombrarlo tal como es, por su nombre, es material de abuso infantil, ningún material podría ser producido sin haber abusado de un niño, la pornografía implica un consentimiento y esto no se puede a aplicar al material de abuso infantil. Entonces yo voy a llamarlo por su nombre, material de

abuso infantil, porque nosotros como policías al tratar con este material no estamos tratando con una foto de una chica de 16 años que se saca una foto en la playa, etc. sino que estamos hablando de niños generalmente por debajo de la edad de diez años que son menores pre-púberes y que son abusados. No somos puritanos que no queremos miren pornografía, sino más bien somos oficiales policiales que tratamos en un entorno internacional para tratar de identificar a estos niños y ponerle un fin al abuso infantil.

La operación Flicker y operación Tornado, Myosis fue una operación que se llevó a cabo en 2006 y 2007 en los Estaos Unidos, trabajó el FBI, también trabajó el Departamento de Justicia, también trabajó la Interpol, más adelante y el Ministerio del Interior de la Republica de Belarus, también la Policía Metropolitana de Londres.

Básicamente estamos tratando con una organización criminal que vende material de abuso infantil, con pagos con tarjetas de créditos Vista o MasterCard, uno puede registrarse on-line, paga el servicio y luego ingresa los detalles de la tarjeta de crédito su domicilio postal incluido y bueno, podría hablarles todo el día del por qué la gente lo hace, pero es tema para otras sesión.

Bien. Se carga toda esta información y se accede al material de abuso infantil en gran volumen. Se utiliza un nombre de usuario y una contraseña que uno recibe. Más adelante la operación Flicker que era la

parte de Estados Unidos y del FBI tomó otro rumbo y ellos adoptaron otra manera de hacer la operación. Acá tenemos la operación Tornado que fue la operación contra el lavado de dinero de la República de Belarus, descubrieron una estafa dentro de su jurisdicción, alguien que estaba generando muchísimo dinero a través de esta operación. La operación Myosis fue la operación de la Policía Metropolitana de Londres, ellos pudieron obtener la lista de clientes o los idiotas que ingresan sus domicilios, sus códigos postales, sus datos de nacimiento, de la tarjeta de crédito, en todos estos sitios web y pagan este material de abuso infantil. Y obviamente era de esperar en un país con servicios policiales avanzados como Estado Unidos, fue justamente el FBI el que rastreó estas compras encubiertas y rastreó a quienes hacían las compras y rastreó los pagos. Básicamente a través de "PayPal", era básicamente una técnica de lavado de dinero utilizando mulas de lavado de dinero a tal fin., etc.

Finalmente Interpol le envió a 140 países registros de pagos de alrededor de 65 mil registros de pagos, realizados por individuos y se los enviamos a estos países para que tomaran las acciones necesarias, algunos países reaccionaron y otro no.

La República de Belarus capturó a esa organización criminal y actualmente están cumpliendo una condena de hasta 10 años de prisión por lavado de dinero.- Era una organización delictiva organizada muy, muy notoria, ellos podrían haber realizado un gran número de actividades ilícitas, uno de los eslabones de esta cadena estaba en ucrania, eta operación se llamó operación "basket", básicamente lo que hacía era tomar contenido de abuso infantil y lo publicaban en la web,

on-line, y esto generó un sistema de abuso del DNS mucho más sofisticado. Cada una de estas operaciones hubiese tenido al menos 2 mil nombres de dominio y en este caso en la operación “basket”, se utilizaba un método creado anteriormente que tiene que ver con la registración de los nombres de dominio al azar. Lo interesante es que de todos esto, 2 mil nombres de dominio tenían datos muy precisos de WHOIS y no se habían pagado con las tarjetas de crédito de esto idiotas que ya mencioné anteriormente, básicamente lo que hacían era utilizar la información que utilizaban estos idiotas para comprar material de abuso infantil y obviamente después la información de WHOIS era totalmente inservible, no tenía valor.

Se utilizó un nombre en general los nombres están correctos, los números de teléfonos están correctos pero es simplemente información que se saca de internet.

Hay muchas medidas para contrarrestar todo esto, si usted tiene o se dirige a través de este mecanismo o es referido a través de este mecanismo entonces va a acceder a un sitio web que va a decir que su cuenta ha sido finalizada. Obviamente la Policía ucraniana estaba investigando este eslabón de la organización delictiva, entonces al acceder a estos sitios web había un menaje que decía “cuenta finalizada”, estaba utilizado el método de inyección directa, utilizados por los “hackers” que utilizaban máquinas que ya estaban comprometidas para desplegar el nombre de dominio, obviamente al ir a ese nombre de dominio era un nombre de dominio inocente cuyo

contenido provenía desde otro lugar. Este otro lugar era generalmente otro país centroamericano o un país del Este europeo y en un solo caso había un archivo en sistema de PH y fue ese archivo pasó a otro servidor, si en un servidor encontramos muchísimas información pero estaba encriptada, este es el nivel de detalles que tenemos que afrontar en estos casos.

El material de abuso infantil en internet ha sido reducido en gran parte, ya no vemos la misma cantidad que se veía antes. Está aquí mi colega de Interpol noruega, que hablará con ustedes acerca de los sistemas de bloqueo en curso en algunos países europeos y en Escandinavia, pero el resultado es que a raíz de la reducción del material a abuso infantil en la web vemos que esto es posible por una solida actuación policial que pudo desbaratar esta organización delictiva gracias a la operación Tornado y cuyo miembros fueron arrestados por las fuerzas policiales y están cumpliendo una condena de prisión.

Con lo cual un buen accionar policial y una mayor capacidad operativa de las fuerzas policiales en todo el mundo lleva a la reducción de este material en la web. Hay una coalición financiera, quizás ustedes la conozcan, opera en Washington D.C., es una organización como “PayPal”, como Visa, como Mastercard, todos se reúnen y discuten estos temas con las fuerzas policiales del mundo, también tenemos una ONG, tenemos un Centro para el tratamiento de niños explotados y desaparecidos y se sabe cuáles sistemas de pago se utilizan y si se detectan un sistema de pago utilizado para o en detrimento de un niño

esta cuenta va a ser cancelada inmediatamente. Hay muchas “hot-line” en todo el mundo, aquí en Estados Unidos tenemos una línea de ciber-seguridad, podemos hacer un llamado y así se bloquean estos accionares y se reduce la cantidad delictiva y de material filmado y de videos en la internet; con lo cual hay menor acceso a este material.

Obviamente que hay un pequeño hoyo, un bache y este bache es el DNS. Hay una falta y tiene que ver con la ICANN, este gran bache tiene que ver con la falta de esfuerzo así que yo insto a la ICANN y a los registradores, me gustaría ver una coalición de DNS de la misma manera que hay una coalición financiera y de esa manera podría haber un proceso para separar o suspender a un dominio que está bajo investigación.

Nosotros tenemos una lista de bloqueo en Interpol y los criterios son muy estrictos per se trata de material que es definitivamente ilegal. Esos 400 dominios, estamos hablando de 400 ó 500 dominios, que tienen niños muy pequeños que participan en actos sexuales, que están siendo abusados, nos gustaría ver un sistema mediante la ICANN o quien fuera tuviese el poder o la facultad de dejarlos sin efecto inmediatamente.

Hay algo interesante el WHOIS preciso o con exactitud, esto parece una especie de broma, porque nunca vemos este WHOS preciso, esto es siempre un callejón sin salida, y realmente no veo el sentido de tener una base de datos de WHOIS si esta base no es precisa, tiene que haber alguien, que esté encargado de esto y por favor le pido que cumpla con su trabajo. Con respecto al gTLD y a los ccTLDs bueno, a veces vemos

ccTLDs que participan en actividades delictivas contra los niños, probablemente sea muy difícil actuar en contra de ellos, yo sé que nosotros vemos distintos tipos de dominio pero puedo garantizarles que en algunos países pequeños donde tienen procesos fuera de control hay cosas que realmente no existen. Nosotros estamos aquí porque queremos llegar a la ICANN, la ICANN llega hacia notros y aún así no podemos comunicarnos. Así que yo diría que nos pongamos a trabajar, manos a la obra.

Aplausos –

Steve Crocker: Gracias Michael y gracias por hablar así y con tanto énfasis y me disculpo por no pronunciar bien el siguiente nombre que es Robert Flaim y yo le digo Bobby.

Robert Flaim: Bueno voy a dejar aquí a mis colegas a Terri Stumme y a mi siguiente colega que hablen antes que yo.

Terri Stumme: Buenos días soy Terri Stumme y voy a hablar sobre la relación que existe entre el sistema de abusos. He trabajado mucho tiempo en el tema en el área de farmacia de la FDA y hace cuatro años que he estado trabajando y nuestra sesión es el principal punto de contacto para las investigaciones a nivel nacional e internacional, en cuanto a las

organizaciones de tráficos cibernéticos farmacéutico. Podríamos decir que tenemos – que las drogas siguen matando a cada vez más personas, mas de 6 millones de estadounidenses utilizan drogas prescriptas y de abuso. En Florida entre el 2008 y 2009, 6 mil personas fallecieron por este tipo de drogas, por sobredosis de drogas. En el Norte de California en junio de w008 a junio de 2099 una persona murió también de sobredosis y desde el 2005 a 2009 la sobredosis de drogas se incrementó en Ohio en un 249% y en Virginia Oeste entre el 2004 y 2009 también se incrementó la sobredosis en un 550%. Del 2001 al 2005, más de 32 mil personas murieron en los Estos Unidos por sobredosis de drogas y esto representa un incremento del 100%. SI ustedes no verifican a sus empleados podemos considerar que entre el 2005 y el 2009 habrá un 40% de incremento de pruebas positivas en los empleados. Es enorme el número y en 2009, 14 individuos fueron condenados de tráfico ilegal en internet de sustancias controladas y esto se ha esparcido en los Estados Unidos.

La compañía (…) más de 78 millones de dólares por la venta de droga mediante sitios de internet, en otra red de farmacias, se identificó que se recibieron muchísimos paquetes, mas de 7900 que contenían 14.400 y más unidades de dosis para drogas de prescripción en un período de diez y seis meses. Internet se ha convertido en una herramienta para el comercio ilegítimo y también se ha utilizado para facilitar la actividad crimina. La DEA y las investigaciones han revelado que hay muchos obstáculos corruptos en internet, que intentan frustrar los procedimientos, los desarrolladores de sitios web y los proveedores de

alojamiento, los registradores de ICANN y los procedimientos siguen aún con posibilidades de mejoras. Incluso si encontrásemos una dirección física para poder actuar, sería difícil, internet y los programas implican miles y miles de nombres de dominios que van activa a otro departamento.

Hemos tenido cambios en la información de WHOIS, transferencias de nombres de dominios lo cual hace que nuestra tarea sea difícil. En 2009 los Estados Unidos estableció un rito de ayuda on line para consumo y la protección en internet y esto implicó el control de sustancias mediante internet. La sección 841H del párrafo señala que en general debe ser ilegal ara cualquier persona que distribuya drogas intencionalmente mediante internet, excepto lo que esté autorizado por el inciso B) y las actividades deben ser controladas que están modificadas. B) Emitir una prescripción para una sustancia controlada con el propósito de hacer una entrega por medio de internet.

Y quisiera enfatizar en la parte c) qué es un agente y qué es un intermediario que causa que internet sea utilizado para encontrar al comprador y al vendedor en la administración de sustancias controladas. Las recomendaciones hechas por la comunidad de ICANN basadas en investigaciones a nivel nacional e internacional y la intención de estas recomendaciones es determinar y frenar los crímenes cibernéticos futuros y presentes. La implementación de los nombres de dominios internacionalizados y el creciente número de dominios de alto nivel

genéricos en el IPv6 hacen que sean necesario continuar avanzando en el monitoreo en sí mismo.

La seguridad y la salud pública están en riesgo. Gracias.

Steve Crocker: Gracias Terry por tus palabras.

Glenn Watson que tiene la palabra ahora.

Glenn Watson: Soy Glenn Watson trabajo para la administración de drogas y alimentos de Estados Unidos y estamos llevando a cabo investigaciones sobre productos aprobados por la FDA en productos farmacéuticos también.

Para no repetir lo que ya se ha dicho, voy a tocar otros temas diferentes a los que dijo Terry respecto del control de sustancias. SI bien se está siguiendo la implementación de la ley, se ha comenzado un gran comercio para la venta y compra de drogas contraladas y también el contrabando. Hubo un estudio hecho por la organización Mundial de la Salud que indica que el 50% de todas las drogas que se vender on line, desde el sitio web, pueden llegar a ser falsas. Cuando uno analiza a las personas que pasa el tiempo y dicen “bueno, están vendiendo Viagra u otras drogas de ese estilo”, pero si uno va más en profundidad hablamos de otro tipo de drogas que son vitales como por ejemplo Lipitor, Crestor, Plavix, Nexium, Zyprexa y productos relacionados con el cáncer.

Cuando uno lo mira desde ese punto de vista es un problema mucho mayor, creo que se está consciente de esto. Uno de los temas que hemos discutido es si los servicios proxys. Son apropiados para organizaciones que venden productos regulados como por ejemplo las compañías farmacéuticas, como si uno fuera a ir al médico o al farmacéutico y cuando uno tiene una receta y puede contactar a esas personas y hacerles las preguntas que necesiten.

Tenemos organizaciones criminales que operan en la internet y que quieren ser contactadas y que también pasan tiempo utilizando los servicios proxy u otros mecanismos para tratar de continuar actuando y hacer que los clientes compren esas drogas. También hemos visto otros temas en los últimos años donde operan sitios web relacionados con productos farmacéuticos y cuando el cliente emite una orden son entonces contactados y se les dice – les dicen al cliente - "usted está comprando droga o están contrabandeando droga" y resulta que es alguien que trabaja para DFBA y nosotros trabajamos para el FBA o FBI y dicen "bueno, si no nos pagan dentro de un determinado tiempo entonces vamos a iniciar un proceso".

Los productos farmacéuticos también son contrabandeados pero además también son abusados y hay información critica de persona que roban dinero para los clientes que compran estos productos on line. Gracias.

Robert Flaim: Soy Bobby Flaim y quisiera decir algunos comentarios para resumir lo que ya hemos escuchado en el panel sobre la explotación infantil, los "botnets" y también el contrabando de productos farmacéuticos.

Lo que hemos hecho es a nivel de la comunidad para establecer recomendaciones en dos partes, una es hacer que ICANN asegure a los registradores y registros dentro del futuro del nuevo proceso de gTLD y que sean mucho más responsables y capaces de lo que son ahora y en segundo lugar, con los registros y los registradores queremos asegurarnos que el registro d los nombres de dominio sean exacto y que no sean delincuentes como ya vimos hoy, que obtienen estos recursos para poder incrementar su actividad maliciosa.

Tenemos muchísima inteligencia actuando en los registros y en la comunidad de registradores pero queremos saber que el 100% de la comunidad lo pueda lograr.

Hoy hemos estado hablando con los registradores y registros para poder proporcionarles las herramientas necesarias y que han aprobado ellos, por eso llamamos a esto recomendaciones, queremos obtener lo mejor de esto para poder abordar los problemas de la mejor manera y la razón por la cual hacemos esto es que hay tantos problemas con los actuales gTLDs que no queremos que esto sea más masivo de lo que ya es en el gTLD y creemos que es momento ahora de tener y resolver este punto. Y por eso esperamos que con estos ejemplos que les dimos y mediante las

recomendaciones trabajemos con ICANN, los registros y los registradores y los miembros de la comunidad para poder lograr este objetivo que todos queremos.

Aplausos-

Steve Crocker: Gracias. Estamos un poco atrasados en cuanto a nuestra agenda, esta es la parte que dedicamos a la sección de preguntas y respuestas, pero hay algo que quiera acotar alguien. ¿Hay alguien que tenga alguna pregunta? Puede acercarse al micrófono, si quiere dirigirse a alguno de los panelistas, si tienen preguntas lo pueden hacer.

Soy de ".com". Tengo una pregunta. Se les requiere a los registradores por contrato que obedezcan con lo que se establece en la ley y en los acuerdos. Y queremos saber si ustedes recién toda la información que este modelo nos plantea a nosotros o no!

Robert Flaim: Como dije, hemos visto un pequeño ejemplo de cooperación pero desafortunadamente hay un tema mayor, que es informarnos y ver qué es lo que podemos hacer en ese caso, y a veces los casos son tan diferentes y los recursos tan poco que no lo podemos resolver o que el método que utilizamos no es el más efectivo.

Steve Crocker: Paul!

Paul Vixie: del Consorcio de Internet. Quisiera agradecerles a todos ustedes por decir lo que quieren decir o por lo que hay que decir que ya se ha dicho antes, pero que nunca sobra.

Voy a decir que ustedes han estado haciendo lo que ya han descripto hace un tiempo, veo que hay un cierto tono de exasperación en sus voces para lo que es la comunidad de ICANN, que cada vez es más grande al igual que la industria y las economías, hay lugar para todo tipo de experimentos que tiene que ver con el "loopholing" o con otras actividades, y esto parece un problema creciente para todos nosotros, entonces, creo que voy a redoblar mis esfuerzos para ver que lo que ustedes piden suceda, espero que otros en esta sala también compartan esta idea conmigo.

Y quería mencionar simplemente y brevemente que otros campos tecnológicos además del DNS tratamos de mantener y de lidiar con estos problemas con un sistema de representación en lugar de seguir tomando acciones dispersas o privadas. Porque nos alejando del objetivo o del sistema inicial. Soy el autor de este sistema, una sistema

tal para el DNS que es el “bind” y seguramente van a haber otros productos similares.

Así que si la comunidad no puede llegar al tipo de responsabilidad que se describen entonces, hay que tomar acción porque si no va a suceder que el DNS va a ser inevitablemente menos confiable, así que les agradezco por hablar tan vigorosamente sobre estos temas.

Steve Crocker: Gracias Paul, Rick

Rick Wesson: Gracias. Rick Wesson. Aprecio todos sus comentarios y comprendo que hacer lo que hacen es difícil. En el 2003 aproximadamente, en la reunión de ICANN que se celebró en Beijing, yo hice un relevamiento de los registradores para autenticar y verificar WHOIS a fin de que todas las entradas se pudieran identificar al momento de la asignación. El costo fue muy bajo por cada nombre de dominio y pudimos cubrir unos cuantos países, 209 países.

Y no fue viable, yo cometí un error, creo que tenía que intentar venderlo y luego implementarlo.

No es imposible, se puede hacer en la actualidad hay servicios que se pueden comprar que son muy baratos, que cuestan centavos y que realmente nos ayuda. Se puede hacer como decía, hay que tener voluntad de hacer algo entre la transacción del registro de los nombres de dominios, pero veremos entonces la expansión de nombres de

dominios totalmente exactos que no tienen conexión, esta brecha es difícil de transitar. No sé si será una estrategia viable que pueda impactar en este problema en particular que hoy tenemos, pero si definiendo la idea de que ICANN tiene un mecanismo que la población en general puede informar a ICANN para determinar estos propósitos en forma estadística y comprender la problemática en profundidad y trabajar en las direcciones IP o en los nombres de dominio. Juntar toda la información requerida para poder llegar al objetivo final. Y creo que ICANN abre la puerta a la comunidad para que intente entender cuál es el problema de la información de este proceso lo cual es sumamente valioso. Gracias.

Steve Crocker: Don!

Don Blumenthal: Soy Don Blumenthal. Soy representante del Registro de Interés Público y también he pasado algo de tiempo trabajando para el Estado.

El ejemplo que se utilizó, si se lo considera desde una perspectiva más amplia, señor Moran, si uno considera a los registros y dice " hay un actor que es erróneo, hay que eliminarlo" entonces - ¿Puede decirme usted que tiene la evidencia? ¿Me puede mostrar la evidencia para hacer esto?

Michael Moran: Mi colega aquí sentado conmigo Bjorn-Erik tiene un criterio muy estricto respecto de qué cosa va a estar incluida en la lista y que todo está disponible para ustedes, para su centro de información nacional, si usted por ejemplo pertenece al FBI o de Botswana o de donde sea. Esa lista será puesta a disposición, para usted o para cualquiera que la necesite, la evidencia está ahí. Si uno está buscando información basada en Francia entonces se va a buscar el canal correcto para que la información sea de Francia y está todo ahí.

Lo que pedimos es simplemente como dije, es que corramos las sillas y nos decidamos a actuar, es decir, nos pongamos a que actuemos. Y creo personalmente que podemos poner e implementar los procesos que nos permitan lograr esto y que podamos finalizar con las investigaciones pendientes. Yo creo que sí es posible cuando hablamos de la seguridad pública y los delitos contra los niños diariamente. Lo único que uno puede pedir y esperar es que las personas se comprometan a realizar el esfuerzo y eso es lo que tenemos que hacer, ese es nuestro trabajo. No hay que dejar pasar cosas y mostrar sólo lo que estamos haciendo, sino que hay que intentar y seguir intentando.

Esto es todo lo que pedimos.

Don Blumenthal: Brevemente, no sé si todo lo que usted dice funciona como tal. Y quizás ese sea el tema, es una de las razones por las cuales los PR han sido tan insistentes. Hemos confiado en un nivel u otro, pero quizás no lo hemos

logrado y quizás haya que revisar la evidencia y ver si existen problemas allí. Habiendo estado en el tema quizá podamos identificar mecanismos para mejorar el proceso.

Glenn Watson: Lo único que voy a agregar es la lista del FDA que nos puede ayudar y que ha sido muy proactiva y que nos ha ayudado y nos ha proporcionado nombres y documentación y que especifica qué leyes han sido violadas en particular, algún alegato que recibimos con respecto a los registradores a los cuales se les suspendió los nombres de dominio fue información importante.

Entonces, ver si se está operando de manera legal y si se está vendiendo drogas de prescripción y si esto viola o no las leyes de los Estados Unidos, es también importante y es algo que tenemos que considerar siempre.

Steve Crocker: Quisiera finalizar este intercambio tan maravilloso de ideas porque el reloj sigue corriendo.

Esto es un intercambio sumamente rico y este intercambio de procesos y de igualdad entre los procesos es algo que nos permite continuar dialogando mientras tanto.

Todos ustedes han hecho un trabajo muy importante, han elevado el nivel de conocimiento y también la temperatura ha elevado, todo esto sobre este tema. Así que permítanme agradecerles a todos ustedes, les

voy a pedir a la audiencia que les agradezca y vamos a hacer entrar al siguiente panel.

BREAK –

(inaudible) de la comunidad de At-large, los otros representantes son de Afilias, Ram Mohan es representante de Afilias, nuestro próximo orador.

Ram Mohan: Muchísimas gracias por este panel. Por darme esta oportunidad. Quiero hablar específicamente acerca de los bloqueos y las cancelaciones o bajas, quiero hablar de algunas experiencias operativas prácticas en Afilias. Como han dicho los oradores anteriores muy claramente y elocuentemente el panorama de los delitos electrónicos, está muy interconectado, hay una cosa que lleva a la otra y hay muchos componentes que funcionan de una sola forma, unidireccional, pero hay componentes bidireccionales.

Quiero decirles que estuvimos haciendo nosotros y compartir algunas de nuestras experiencias. Las bajas en nuestra experiencia funcionan, por ejemplo el ".info" fue institucionalizado como una política anti abuso en colaboración con los registradores en octubre de 2009. Seguimos un

proceso de comentarios públicos de la ICANN, seguimos ese sistema y los registros son el punto central del análisis y de la diseminación de datos y Afilias ha forjado varias relaciones con la comunidad de la seguridad, también tiene relaciones con la comunidad de registradores, pero el método fundamental que estuvimos utilizando es el siguiente, se reportan los problemas a los registradores quienes consideran dar de baja a los nombres que le son referidos y las bases son que los registradores tienen una relación con los registrantes y el registrador está en una buena posición de hacer cumplir el contrato del registrante. También tienen datos superiores en comparación con los registros. Los registros que nosotros operamos son registros técnicos pero son registros muy extensos, muy amplios, pero los datos que tenemos no son tan buenos como los datos que tienen los registradores. Entonces esa es una de las bases.

Con respecto a lo que ha sucedido a octubre de 2008 a la fecha hay más de medio millón de nombres de dominio de ".info" que han sido reportados a los registradores pero han sido objeto de acción por parte de los registradores o bien han sido dados de baja.

Con respecto a la política anti abuso de Afilias para ".info" el registrador tiene la capacidad y la facultad de actuar pero en general no tiene porque hacerlo.

Con respecto a los principios de éxito, en primer lugar las bajas funcionan porque se abocan a un problema desde la fuente y las bajas son específicas y son una respuesta directa. Sin embargo, a menudo uno actúa a nivel atomizado y no necesariamente a gran escala, con lo cual si uno tiene un registrante en particular o un elemento delictivo que utiliza el nombre de registros que utiliza un montón de tácticas, entonces uno a la larga se ve forzado a actuar caso a caso o nombre a nombre, lo cual puede ser engorroso y bastante lento.

El bloqueo de los DNS consta de lo siguiente.

En primer lugar quiero definir qué quiero decir cuando digo bloqueo. Para mí es la forma de no permitir que se lleven a cabo los pedidos de información de los DNS, tiene que ver con la suspensión de un nombre de dominio eliminándolo de una de las zonas. Entonces en el caso de los bloqueos de los DNS son válidos pero necesitamos una metodología para garantizar que no se cumplan estos pedidos de información. Los bloqueos pueden ser una respuesta desproporcionada al problema en sí mismo.

Si vemos el tema "spam" por ejemplo, veremos que esto sucede a nivel de organización local y como dijo el orador anterior, tenemos listas negras que podemos utilizar. Pero si vemos el DNS vamos a ver que básicamente todo depende del DNS no sólo los sitios web si bien son los componentes más importantes. Con lo cual hay varias preguntas con respecto a si el bloqueo es realmente el curso a seguir.

Es mi opinión personal que bloquear un TLD a nivel del productor de servicios de internet o más arriba puede ser algo realmente desastroso con consecuencias no intencionadas.

Claramente se puede crear confusión para los usuarios de internet porque es difícil comprender quién es el responsable y cómo corregir el problema. A menos que tengamos un nombre real no sabemos a quién hemos bloqueado, a quien tenemos que recurrir, no queda muy claro. También es incompatible con el DNSsec a muy alto nivel, el DNSsec interpreta estas mentiras como intentos de intrusión y socaba los esfuerzos de generar confianza en todo el sistema de DNS. También hay daño colateral que tenemos que tener en cuenta y tenemos que ser muy cuidadosos al respecto.

Estos son algunos pensamientos acerca del bloqueo y los resultaos de dar de baja a los DNS.

Gracias.

Steve Crocker: Muchas gracias. Christine, es la próxima oradora.

Christine Jones: Gracias Steve. Soy Christine Jones represento a Go-Daddy. Nosotros abordamos el abuso al DNS a diario y de distintas maneras, en varios contextos.

Siempre me gusta comenzar diciendo que los nombres de dominios no cometen delitos. No lo hacen, la gente que registra los DNS a veces comente delitos y no queremos ser parte de su operatoria delictiva. Estoy – discúlpenme – si me pongo los anteojos, estoy adaptándome a los anteojos. Me los voy a quitar Ahora sí, todo se ve maravilloso.

Nosotros trabajamos con Interpol, con la DEA, con la FDA, trabajamos con ellos a diario, porque lamentablemente la gente mala existe en todas partes, independientemente del "spam", de la pornografía, o como dijo el colega irlandés, el "abuso infantil" porque de eso se trata, nosotros enfrentamos estas cuestiones a diario y adoptamos un enfoque mucho más agresivos que otros registradores, pero nosotros tenemos 1.6 dominios por segundo realmente, y tengo más o menos 100 personas que trabajan 24 horas al día siete días por semana ocupándose de estas cuestiones y sé que esto es algo único en este ecosistema. No todo registrador cuenta con 100 personas que trabajan 24 horas los siete días de la semana.

Con lo cual al pensar cómo abordar estas cuestiones tenemos que ver cuál es la escala, la magnitud de este registrador, qué puede hacer, cuánto peso tiene su envergadura en la solución del problema. Creo que todo registrador que es ciudadano corporativo legítimo estará de acuerdo en lo siguiente. Si uno tiene que tener infraestructura tiene que respaldar la lucha contra el abuso al DNS. No todo el mundo te puede responder Bobby dentro de una hora como lo hacemos nosotros. Esto forma parte de mi agenda política e representación de los registradores,

pero en fin, para nosotros es muy exitoso tener un enfoque híbrido para afrontar el abuso al DNS en una variedad de contexto.

Nosotros tenemos legislación que nos permite abordar actividades que hace que el abuso al DNS sea ilegal con lo cual los organismos de cumplimiento de la ley, nos permite ir detrás de los malos de la película, por así decirlo, además unimos esto con la cooperación voluntaria con miembros de la industria.

Necesitamos contar con la colaboración voluntaria porque los organismos de cumplimiento de la ley, simplemente no cuentan con los recursos para rastrear a cada "spammer" que registra un nombre de dominio por menos de 10 dólares, realmente no se cuenta con esos recursos.

Y corríjanme si me equivoco pero sirve mucho más trabajar afirmativamente y proactivamente y darle de baja a alguien que sabemos que está cometiendo un acto delictivo simplemente con una notificación de los organismos de cumplimiento de la ley en lugar de realizar toda una investigación.

Este enfoque ha funcionado muy bien en los Estados Unidos, hemos trabajado exitosamente con los organismos a cargo del cumplimiento de la ley el FTC, el FCC los organismos de cumplimiento de la ley que realmente no cumplen funciones de Ministerio Público, en este rubro.

Hemos trabajado con ellas independientemente de temas de drogas, d medicamentos falsificados o con venta bajo receta, de pornografía, todas estas cosas que se han mencionado.

A nosotros no nos interesa que se utilice nuestro sistema para que la gente pueda cometer delitos en internet. Esa no es la razón de nuestro existir, a menos y hasta tanto todos los registradores cumplan con una norma que indique que hay que hacerse cargo de la gente de mala fe en nuestro sistema, no importa cuanto pueda trabajar GO-DADDY y cuanto pueda trabajar otro registrador para solucionar el problema, nunca podremos solucionarlo porque siempre habrá un grupo de registradores que sea una especie de refugio para toda esta gente y nosotros tenemos que solucionar este problema. Muchísimas gracias.

Aplausos –

Steve Crocker: Gracias Christine. Marc! Marc creo que usted sigue.

Marc Rotenberg: Yo soy Marc Rotenberg, pertenezco al Comité Asesor At-large. Soy también Director del Centro de Información Electrónica de Washington y también asesoro al Congreso y algunas otras organizaciones internacionales respecto de temas relacionados con la seguridad y las libertades.

Y en cuanto al abuso del DNS es un tema muy significativo para la comunidad y apoyamos en DNSsec y consideramos que es necesario para el cumplimiento de la ley que siga avanzando en políticas para evitar el mal uso.

Pero creo que hay un punto que tenemos que entender y conforme avanza esta conversación. Hay otra serie de preocupaciones que tengo que traer a colación. Una es que se ha mencionado muchas veces, tiene que ver con la Justicia o el debido proceso del proceso de cumplimiento de la ley.

Si uno está bajo este proceso o si está monitoreando debe saber que la decisión que se tome tiene que estar justificada y debe ser correcta. Y se debe abordar el tema particularmente conforme los gobiernos se responsabilicen más y tienen más acceso al tema de abuso del DNS, porque hay muchos encuentros entre las personas con buenas y malas intenciones. Y creo que Christine ya hizo un punto al respecto. Es importante que los participantes entiendan cuáles son las reglas y se deben proporcionar algunas pautas para que puedan saber cuándo y cómo tienen que responder, cuál es el período para hacerlo para que puedan responder como se les pide. Y creo que es aquí donde hay que proporcionar clarificación conforme avanzamos en el tema del DNS.

También hay preocupaciones o temas relacionados con el crecimiento de las atribuciones on line y el DNS ha proporcionado una mejor

autenticación pero también la comunidad necesita considerar las atribuciones de los usuarios finales; porque es posible rastrear las actividades de usuarios específicos y entonces hay una nueva manera de perseguir o ir detrás del abuso y abrir al capítulo del IPv6 seguramente podamos hacer uso de estos dispositivos y herramientas y estos son posibilidades futuras, pero desde la perspectiva de la privacidad creo que vamos a considerar el interés del usuario final que todavía no hemos tocado tanto, tenemos que llevarlo a nivel del consumidor, a nivel del usuario, porque aquí también se encuentran algunos riesgos importantes.

Gracias.

Steve Crocker: Gracias Marc por su comentario. Ahora le vamos a dar la palabra a Bjorn-Erik.

Bjorn-Erik Ludwigsen: Voy a decir mi nombre yo mismo que es Bjorn-Erik Ludwigsen. La razón por la cual suena tan extraño es porque soy un agente de Interpol que trabaja en Francia y también estoy relacionado con el acceso y bloqueo de acceso de los nombres de dominio.

Así que voy quizás a estar en desacuerdo con el primer orador de este panel. ¿Qué es lo que bloqueamos? Bloqueamos porque pensamos que

prevenir es mejor, y al razón por la cual yo quiero prevenir los crímenes o los delitos es porque quiero prevenir que haya víctimas.

Yo no ´se nada respecto del "phishing", "spam", yo lo que sé es de crímenes o delitos analógicos, sé también del abuso infantil que es un delito análogo y entonces esto es análogo y también lo son las víctimas.

Queremos prevenir el delito mediante el envío, recepción y visión de material que ha estado circulando, la exposición de este material a la comunidad quizá puede parecer demasiado estúpido pero estamos haciendo lo mejor que podemos para evitar que siga circulando la pornografía.

Comenzamos esto en el 2004 en lo que era la edad de piedra para internet, donde ya había material de abuso infantil dando vuelta en el sistema. También hubo una lista en nombres basada en la legislación de Noruega y países como por ejemplo Escandinavia que emitieron legislación al respecto. Y esto es algo a lo cual se puede tener acceso. Primeramente nos gustaría ver que todos los países tengan sus sistemas de bloqueos, sus propias leyes que les digan a los proveedores de internet qué es a lo que pueden acceder en ese país. Estos son los países que actualmente tienen un sistema de policía operando, algunos otros países son países que se llaman países Circamp, como por ejemplo tenemos a Noruega, Suiza, Dinamarca, Finlandia, Italia o Nueva Zelanda, así que vamos a tener evidencia de esto también.

Ellos pueden utilizar sus leyes y bloquearlo de acuerdo a esas leyes.

Pensamos entonces que esto fue una buena idea y pensamos que todo el mundo lo aceptaría y que realmente sucedería, entonces, lo que necesitamos hacer es que se transforme en legal para todos. Esto se presentó en la Asamblea General en Singapur en 2009 y fue aceptado por todos, hubo una aceptación unánime. Básicamente esto significa que todos los jefes policiales presentes en aquella reunión estaban dispuestos a utilizar medidas técnicas para limitar el abuso infantil y pensaron que era una buena idea en aquel entonces.

Estos son los criterios de los que se hablaron, pero necesitamos escuchar algo que sea legal en todo momento, incluso en los países que son más seguros. El problema es que en la mitad de los países del mundo, el material de abuso infantil, no está definido en las legislaciones y no puede entonces por lo tanto ser considerado como tema de pornografía infantil. Entonces decimos que si consideramos a un niño como una persona menor de 16 años y queremos que sea la edad se baje a 13 y asegurarnos de que sea realmente un niño para que no haya otro tema relacionado.

El abuso severo es algo que tiene que ser definido en el código penal de cada país y se tiene que dar una focalización más determinada o específica al respecto.

Estos son las agencias policiales que específicamente tiene una sección dedicada al abuso infantil, esto está hecho de acuerdo a ese criterio.

(inaudible) y tiene que estar on line en los últimos tres meses, los mantenemos así porque vemos que a veces vuelven, se van, el alojamiento se elimina y luego en dos meses vuelven a parecer y a seguir funcionando.

En 2011 hemos tenemos en realidad una lista de nombre de dominios que es de 386 y hubo un incremento desde esa segunda parte del 2010 hasta el 2011 de una duplicación del número de nombres de dominios. Generamos esta lista y la pusimos a disposición de todos, ya sea que uno sea un proveedor de servicios de internet o no, puede utilizar esta lista para tratar de limitar los canales de distribución en la red, y está disponible en forma gratuita contiene datos estadísticos y se puede conseguir mediante las oficinas de policía, como por ejemplo la Interpol. No se nos tiene que dar nada a cambio, vamos entonces a poner una página disponible que no es obligatoria pero que uno puede ahí registrarse y sugerir si es necesario, algo para tratar de frenar el abuso infantil. Estos son los tipos de dominios que tenemos actualmente, son más de 386, algunos de ustedes quizás lo reconozcan, algunos quizás sean responsables de estos dominios, no estoy diciendo que algunos sean mejor o peor que otros, ".com" es el más abusado, luego tenemos a aquellos que pueden lidiar con este tema de dominios de alto nivel y disminuir el número de abuso en su país. Pero hay que hacer algo con aquellos países y registros que no pueden disminuir el número de abuso. No les voy a mostrar ningún ejemplo de abuso sexual o infantil, pero sí quiero mostrarle cuál es el material que se utiliza para que vean cómo es y de qué se trata.

Van a escuchar ustedes hablar de actores malos o contenido malo, estos contenidos son los que se distribuyen por internet y muchas personas utilizan estos contenidos para tener fantasías sexuales, masturbarse o simplemente para pervertir a los niños.

Si ustedes ven la diversidad de este sitio pueden ver que tiene muchas imágenes y esto lo tomamos hace unas semanas, y es un problema que tenemos en muchos dominios, si ustedes quizás van a sus computadoras y si se conectan a la red pueden ver esto en su forma original, está disponible para todos ustedes en cualquier momento. Y aquí tenemos una niña de cuatro años de Estados Unidos y su padre abusó de ella y también de su hermanita y bueno, estuvo colocada aquí la foto. Y lo que tratamos de hacer es protegerla mediante la no distribución de su foto.

Una solución parcial es el bloqueo, la última solución es borrarlos pero una y otra vez tenemos el mismo problema, cada vez hay más y nuevos dominios borramos y borramos pero no siempre funciona.

Esta es la página de alto que van a ver cuando ingresan a estos sitios que redirigen nuestro tráfico y se muestra este sitio y se va a explicar qué es lo que sucede y la legislación y si uno es dueño de un nombre de dominio entonces uno se puede quejar o recurrir a Uropol u otro lugar.

Rápidamente voy a hablar de la confiabilidad de WHOIS y de algo que escuchamos siempre. Hay unos ejemplos aquí que podemos ver que lo

que el WHOIS ve lo que no ve. Este es un sitio que encontramos y esta es la información que nos da WHOIS. Vean la información que nos da.

Es aparentemente una persona que administra una compañía financiera en California, esta es su casa, esta es la dirección y el teléfono que corresponde a un Centro Médico en California y el fax que nunca se ha visto. Entonces para nosotros esto significa que no hay información útil y lo que me sorprende es que usted le da un servicio a esta persona en WHOIS y no tiene idea de quién es. ¿Le da información vaga y ustedes los dejan tener acceso a internet?

¿Bueno sin verificar nada lo hacen?

Bueno, pero tenemos que tener en cuenta que si uno da un número de teléfono esto es imposible de chequear, chequear todos los dominios implica que va a haber siempre información errónea para encontrar. Esto es algo que hice yo mismo que quizá podamos discutir o considerar, cuando las personas registran los nombres de dominios, o cuando por ejemplo se roba o sea hace con una tarjeta puede ser con una tarjeta que haya sido robada, entonces, hay que comenzar a rastrear y a verificar las transacciones. Se puede también utilizar la suspensión de los dominios. Tener un dominio en internet no es solamente un derecho humano.

Uno debe saber cuáles son las reglas y si no las cumple simplemente se suspende y si no se soluciona entonces se borra. Si no tiene una dirección de correo electrónico que funcione entonces, yo ya sé que

ellos lo han dicho, pero simplemente habría que borrarlo y ahí si nos evitaríamos muchos problemas.

Debería haber más demanda de personas que tienen dominios o una serie de dominios que están distribuyendo información de abuso infantil ¿Y si se tiene un dominio de alto nivel que hace entonces?

Simplemente hay que suspenderlo.

Si no se sabe qué es lo que se está almacenando no se puede continuar.

Hay mucha información que actualmente está dando vuelta y que podemos proporcionar a las personas que realizan el alojamiento para que verifiquen el material y la información y que se pueda actuar de manera rápida en caso de que haya que suspender a alguien.

Creemos que el contenido on line debería seguir las mismas reglas que el contenido off-line y si no se acepta en la vida real ¿Por qué lo vamos a aceptar en internet? ¿No es cierto?

Y la internet simplemente es parte de la vida también. Es como por ejemplo el agua, o cualquier otro medio o cualquier otro bien.

Gracias a todos por su atención.

Aplausos-

Steve Crocker: Gracias. Tenemos algo de tiempo disponible para preguntas y respuestas si alguien quiere acercarse y hacer alguna pregunta puede hacerlo.

Ram Mohan: Steve ¿Podría hacer una pregunta rápida? En los puntos anteriores a considerar usted dijo la suspensión del TLD en la lista, espero que usted haya querido decir la suspensión de los dominios de segundo nivel.

Bjorn-Erik Ludvisgen: No, yo también soy un ser humano y me puedo equivocar, quizá usé la terminología errónea perdóneme. Lo que hay que hacer es por qué si hay información errónea suspender el nivel o no suspender el dominio entonces, usted no quiere suspender el ".com"

No. No quiero suspender un ".com", nadie va a sacar ".com" todos lo usamos al ".com" en realidad.

Bueno a ver por ahí.

Ben Wilson: Soy Ben Wilson. Cuando hay un contrato con los registradores que es antiguo quizás no sabemos si hay una posibilidad de cambiar el marco respecto de la forma en que esos registros operan. Es esto así con los contratos antiguos?

Margie Milam: Voy a responder eso. El acuerdo de acreditación de registradores es un acuerdo que se firma con los registradores y se actualiza a menudo y el

Consejo del GNSO está actualmente, actualizándolo y hay mucha discusión al respecto de esta actualización.

Es un proceso difícil les voy a decir.

Steve Metalitz: Steve Metalitz de la Colaición de responsabilidad on line y quiero agradecer al panel y al panel anterior por su exposición que fue excelente y también creo que lo que dijo Christine es muy importante. Es importante el cumplimiento a nivel nacional e internacional y también del sector privado.

Pero creo que la pregunta difícil sería ¿Cuál es el rol de ICANN? Y otro vez tomando algo que dijo Christine, si uno no hace que todo el mundo se suba a este barco para seguir avanzando y si esto no se hace a través del acuerdo de registradores entonces, necesitamos un acuerdo que sea mucho más sólido como ya se mencionó, necesitamos un acuerdo de acreditación de registradores más fuerte en muchas áreas y necesitamos un cumplimiento más fuerte por parte de ICANN.

Creo que estos son puntos difíciles de alcanzar pero quizá esta sea la contribución que ICANN pueda hacer a este gran proceso.

Steve Crocker: Gracias. Bueno miren la cola que tenemos, es mucho más larga de la que esperaba.

Malcom Hutty: Gracias. Yo represento a los ICI SP. Hay organizaciones diferentes que representan los registros y registradores y yo percibo algunos temas en común aquí y cuando las agencias de cumplimiento ven que hay acciones erróneas lo que hacemos es que tenemos temas en común que tenemos que considerar.

Esto ha sido una sesión muy interesante al igual que la anterior y me gustaría agradecerles a todos los que expusieron pero en ambas sesiones hemos escuchado respecto de algunos documentos o de acciones que se están tomando y que requieren y rapidez y al mismo tiempo los intermediarios son también responsables de la representación del interés público, de los intereses de la sociedad civil y de los intereses corporativos, entonces tienen que se más fuertes y hay que buscar soluciones para estos servicios y determinar quién es el responsable y quién va a ser el registrador y en nuestro caso por ejemplo cuál va a ser el cliente que vamos a tener.

Entonces mi pregunta para el panel sería. ¿Cómo vamos a equilibrar todo esto? ¿Qué respuestas nos pueden dar para solucionar esto bajo lo que es la confidencialidad y en relación que existe entre el intermediario y las agencias de cumplimiento de la ley? ¿Se puede equilibrar esto a fin de asegurar que haya una visión general de todas las búsquedas, es decir que se cuide el interés público y también el del cliente? ¿Qué salvaguardas o qué protecciones creen ustedes que se deberían

implementar para cuidar a los registradores de estas conductas injustos o delictivos?

Steve Crocker: Christine.

Christine Jones: Bueno. Voy a responder rápidamente. Hay muchos registradores y proveedores de “hosting” así que nosotros hacemos ambas cosas y vemos ambas caras de la moneda. Estamos pendientes sobre los nombres de dominios y también sobre otros temas.

A mí me encantaría enviarle una copia de nuestro procedimiento operativo que responde exactamente su pregunta y que debería tener todos los proveedores de internet y todos deberían seguir. Pero creo que la respuesta a su pregunta es que uno tiene que tener y usted es miembro de una organización, que debe tener un procedimiento que responda a esa pregunta o al problema antes de que el problema surja.

Les voy a dar un ejemplo. Uno tiene que saber cuál es la respuesta antes de que uno tenga la pregunta.

Hay ciertas cosas que “per se” son ilegales, uno puede considerar algunas de las imágenes que hemos visto como ejemplo y obviamente hay algo malo en estas imágenes, pero nuevamente, el equilibrio está en la posición que nosotros tomamos con respecto a los temas. Tenemos que tener algo y tenemos que comprometernos si es que lo vamos a hacer. Lo que uno no puede tener un nombre de dominio si no tiene

control del contenido. Hay situaciones extremas que quizás van a redirigir al DNS es un tema controvertido, uno tiene que tener un equilibrio.

Si yo soy un registrador pequeño me tiene que decir ¿Quién es? Como se opera a nivel legal y qué riesgos se van a correr. Ustedes saben, yo soy muy directa en esto. A mí no me gusta tomar riesgos, pero sé que tampoco quieren tomar riesgos y que otros registradores tampoco pueden tomar riesgos. Pero para quienes no sufren el abuso infantil o el abuso del DNS de manera importante denos alguna ayuda. Eso es lo que les estoy diciendo, ese es mi mensaje.

Steve Crocker: Marc!

Marc Rotenberg: Quiero dejar una idea, veo que tienen bastante sesiones acerca de este tema, del abuso del DNS y sugeriría que – o me atrevería a decir que vamos a hablar mucho al respecto en los próximos años- con lo cual me parece que sería bueno tener cierto tipo de datos, algún tipo de informe anual, por parte de los registradores y que nos indique por ejemplo las notificaciones de bajas de nombres de dominio, un informe o por ejemplo todo lo que tiene que ver con tema de “copyright”, todo lo que tiene que ver con este tipo de temas porque estamos hablando de estadísticas y eso sería muy útil para la comunidad porque entonces,

uno puede tener un sentido de las respuestas de los registradores sobre la base de la ubicación geográfica.

Me gustaría ver cuáles son las tendencias, yo estoy muy familiarizado con estas prácticas desde hacer 30 años venimos viendo cómo las organizaciones privadas responden a solicitudes similares y esto puede funcionar bastante bien aquí. Sería de mucha utilidad tener esta información.

Steve Crocker: Tengo una pregunta. Estos datos incluyen no sólo las solicitudes sino las evaluaciones acerca de si hubo errores de tipo 1 o tipo 2?

Bueno supongo que los de tipo 2 si se registraron.

Marc Rotenberg: Yo quisiera que fuesen lo más objetivos posible, es decir, cuantas solicitudes recibieron, cuantas fueron procesadas.

Bueno pero si hay una objeción posterior y luego se descubre que hubo un error entonces esto no sería muy apropiado.

Steve Crocker: No quiero quitarles mucho tiempo, quiero seguir avanzando.

Ram!

Ram Mohan: Quiero agregar algo más. Uno se atrevería decir que es muy difícil y básico poder brindar un servicio, llevar adelante una empresa, pero realmente no se ve esto muy a menudo. En algunos casos queremos hablar con los proveedores de servicios y solicitarles que den de baja a los nombres de dominios y queremos investigar y realmente se sorprenderían muchísimo al saber que no contamos con correos electrónicos que funcionen o que reboten, que no tenemos números telefónicos, a veces enviamos mensajes y la respuesta que obtenemos es un mensaje de respuesta automática como los que dicen, “estoy de vacaciones” o “estoy fuera de la oficina”.

Esto tiene que ver con el abuso, hay que trabajar bien, apropiadamente, tenemos que contar con medidas básicas, estos son proveedores de servicios y realmente estamos hablando de un daño real ocasionado, con lo cual esta cuestión básica realmente no existe en el ecosistema actual.

Paul Vixie: Gracias. Steve. Como operador de un sistema de servicio de un correo electrónico y de muy buena reputación sé que mucha gente me decía que era muy caro para ellos poder chequear la seguridad de los permisos para la información, era muy caro para ellos controlar los registros de la reputación de las partes involucradas con lo cual, ellos externalizaban sus quejas con respecto a los costos y se externalizaba a la comunidad, no les estoy echando la culpa, sé que la comunidad también ha respondido o tiene un nivel natural de respuesta. Estoy de acuerdo con Ram, el bloqueo es terrible y es algo que no tendríamos que

hacer, estoy aquí para decirles que se está realizando y se va a realizar mucho más ampliamente si la internet sigue multiplicándose a razón de millones.

Entonces quizás podamos ver cambios draconianos a nivel regulatorio de la ICANN.

Quisiera decir que durante mucho tiempo fue el CTO de una empresa y el Presidente de Paix y cuando alguien hacía algo incorrecto personalmente los desconectaba directamente; y no me afectaba la rentabilidad en absoluto.

Bill Smith: Hola Soy Bill Smith de PayPal. También soy miembro del equipo revisor de WHOIS. Quiero hacer eco de los comentarios previos acerca de la calidad de los panelistas, realmente son excelentes.

Con respecto al bloqueo PayPal respalda fuertemente no hacer el bloqueo. No estamos a favor del bloqueo. Nosotros estamos preocupados acerca de los diez años que nos ha llevado llegar al DNSsec y realmente hay un impacto muy negativo que se deriva del bloqueo si se lo utiliza en cualquier modo. Entonces hay que ser muy cauteloso al hablar acerca del bloqueo.

También quiero comentar acerca del abuso infantil. Realmente tendríamos que avergonzarnos como comunidad al permitir que este material siga estando disponible y peor aún, que tengamos sistemas que

hemos implementado y que redactemos políticas respecto a estos sistemas y que sean tan ineficaces que permiten literalmente que se haga casi imposible contactar a las partes responsables.

Realmente me complace mucho escuchar a Go-Daddy hablar de su deseo de no formar parte de estos elementos delictivos, creo que es realmente algo digno de alabanza. Hay una pregunta que tengo. ¿Qué están haciendo Go-Daddy y los demás registradores serios al momento, para cambiar el sistema, para mejorar el sistema de manera tal que los datos de WHOIS sean más precisos y podamos abordar toda esta cuestión que estamos viendo?

Christine Jones: Parece ser una pregunta dirigida a mí. No sé me da la sensación.

A lo mejor podamos hacer esta conversación off line, no quiero hacer una publicidad acerca de Go-Daddy, pero yo destino mucho más dinero, mucho más que PayPal incluso para lograr que el Congreso apruebe una buena legislación al respecto. También trabajo con los agentes policiales para ayudarlos a detener a los delincuentes.

Go-Daddy trabaja con tu gente también y con todos los demás proveedores de servicios de pago vía tarjeta. Nosotros trabajamos con respecto a pornografía infantil como sabrás. Hoy en día es muy difícil pagar a través de PayPal y obtener pornografía infantil fue muy difícil pero lo logramos. Hay muchas cosas que estamos haciendo sobre todo con WHOIS.

Ustedes aquí han hablado acerca de los datos de WHOIS, la mala información de WHOIS durante diez u once años, cada vez que doy una presentación en una Universidad, en un seminario de negocios, en cualquier foro que no sea un Seminario de la ICANN, les digo a la gente: Si ustedes pueden legítimamente verificar los datos de WHOIS se van a volver multimillonarios, porque todo el mundo va a comprar ese sistema y lo va a utilizar"

El caballero de Interpol nos dio un ejemplo perfecto de por qué el verificar los datos de WHOIS en la forma en que se verificó en ese caso, es una mala idea, porque resultó en que él buscara datos de buena fe que eran datos de otra persona y esa no es la respuesta correcta, ojalá fuese inteligente como para poder darte la respuesta correcta pero bueno, lo voy a dejar en las manos del grupo de trabajo de WHOIS.

Si pudiera seguir con mi pregunta, por favor.

Bill Smith: Si con todo respeto este no es nuestro trabajo como equipo revisor. Nuestro trabajo es revisar la política existente y ver cómo se la implementa de manera eficaz. Ese es nuestro trabajo.

Si nos estás pidiendo que forjemos una política, ese no es nuestro trabajo, personalmente con todo gusto sugeriría políticas. Pero como miembro del equipo revisor esa no es mi tarea, con lo cual la pregunta

es ¿Qué estás haciendo individualmente y colectivamente como registrante? Porque veo a los registrantes que colectivamente se resisten a muchos de los cambios para mejorar la exactitud de los datos de WHOIS.

Steve Crocker: Sin dudas este es un tema muy controvertido que viene estando presente desde hace mucho tiempo. Yo desde el Comité Asesor de seguridad y estabilidad he visto como se trata este tema desde hace un tiempo ya y es frustrante ver la falta de progreso, no sólo con respecto a la exactitud sino a la aplicación de esta información y todo lo que tiene que ver con la claridad de los registros. No lo vamos a solucionar aquí y ahora con lo cual voy solidarizarme muchísimo con usted, pero voy a tener que avanzar.

Necesitamos obviamente planificar y hacer un cronograma para que esto se plasme y se pueda llevar a cabo.

Si hay algún tipo de obstáculo hay que sortearlo.

¿Quién es el próximo orador?

Estamos bastante atrasados con el tiempo, pero quiero aplaudir a todos nuestros panelistas, nuestros oradores por su excelente trabajo. Y un aplauso muy, muy especial para Margie que es personal de la ICANN. Margie Milam una superestrella de la ICANN.

Muchas gracias.