PRAGUE – Forum on DNS Abuse
Monday, June 25, 2012 – 16:30 to 17:30
ICANN - Prague, Czech Republic

…….lo más pronto posible. Gracias.

Margie Milam: Hola a todos. Vamos a comenzar con el Foro del DNS y el abuso del DNS. Mi nombre es Margie Milam y voy a ser la moderadora y le voy a dar información sobre el tema. Y voy a presentar a Ondrej Filip quien va a ser el moderador de este Foro.

Ondrej Filip: Bienvenidos a todos. Creo que todos estamos interesados en cuanto a los nombres de dominio y a mejorarlo. Sabemos que internet no es solamente un ámbito para las buenas personas sino que también tenemos algunas personas malas que interactúan. Entonces, este Foro va a hablar sobre el abuso del DNS que es el lado oscuro del ciberespacio.

Tenemos un panel de discusión en este tema. A mi derecha tenemos a panelistas y expertos de mucho conocimiento. Y vamos a tener tres presentaciones, la primera va a ser llevada a cabo por Martin Peterca, luego por Branko Stamenkovic y la tercera va a ser llevada a cabo por Christopher Landi.

La primera va a ser llevada a cabo por Peterca y él es el jefe o Director del “cz.nic” y nos va a contar cómos e trata el tema del Abuso del DNS en este país y cómo interactúan con las agencias y demás.

Así que Martín le cedo la palabra.

Martin Peterka: Buenas tardes. Gracias por presentarme. Hoy voy a decir algunas oraciones sobre "cz nic" y les voy a presentar a nuestro equipo de seguridad y les describiré parte de algunos incidentes interesantes que hemos resuelto en el pasado, al final de mi presentación.

Me gustaría presentar al Gerente de nombres de dominios que también es proactivo. "cz nic" es una asociación que se fundó en 1998, con doce compañías checas líderes y tenía un número de miembros y ahora tenemos más de cien miembros. Tenemos más de 50 empleados y nuestra actividad principal es operar el registro "cz.cz".

Hemos firmado un memorando de entendimiento con el Gobierno checo, y hemos firmado un memorando de entendimiento con las agencias de seguridad que se focalizan en la seguridad, o en el rol del CSIRT de la República Checa.

Somos una organización sin fines de lucro y tenemos una serie de actividades que llevamos a cabo.

Tenemos nuestro propio centro de capacitación, tenemos un Departamento de laboratorio donde desarrollamos software. Y por supuesto tenemos un equipo de seguridad.

Oficialmente "cz nic" tiene dos equipos de seguridad. El primero es un equipo interno, es el "cz nic csirt" que tiene roles principales. En primer lugar, tiene como objetivo el desarrollo de un sistema autónomo. Dado que no tenemos clientes el sistema autónomo son nuestras propias redes. Y es algo bastante simple. Generalmente no presentan incidentes en nuestros programas. Pero la segunda parte, o segundo rol, es un poco

más complejo desde otro punto de vista porque se relaciona con los registros. Nuestro equipo puede desactivar a los dominios que tienen un contenido dañino.

Hablamos de virus, hablamos de malware, hablamos de “phishing”, hablamos de los “podnets”. Si encontramos algún sitio con contenido dañino entonces desactivamos a este dominio durante un mes y si es necesario lo podemos hacer en forma repetida.

El segundo equipo de seguridad opera al equipo CSIRT nacional. Operamos desde el 1º de junio de 2011, y desde entonces el equipo fue liderado por diferentes personalidades, entre ellas el Ministro del Interior y esto llevó que al final de 2011 “CZ NIC” continuaría con la operación de su equipo.

Comenzamos entonces con la operación el 1 de enero y hemos comenzado a transferir la agenda a una empresa distinta.

Desde el 1º de junio de 2011 estamos en total operación porque hemos recibido o estamos recibiendo todavía colegas de SESNET.

Los incidentes se pueden informar y puedo decir que tenemos éxito al hacer esto, pero también tomamos pasos con medidas proactivas. Por ejemplo en la segunda parte del año pasado analizamos datos del DNS autoritativo, para los nombres de dominio y se encontró que la seguridad del DNS se resolvió mediante los puertos estáticos. Y tuvimos administradores de los servidores con los cuales les ofrecimos ayuda.

Dado que algunos de estos resolutores operan en las redes gubernamentales, operamos este proyecto con el servicio de seguridad e información checo.

Nuestra actividad es por ejemplo, organizar reuniones comunitarias, talleres para la comunidad, y tenemos procedimientos especiales donde nos focalizamos en la seguridad en nuestro centro de innovación.

También cooperamos con organizaciones internacionales, u organizaciones como por ejemplo Terena, entre otras.

Terena fue introducida en octubre de 2011.

Aquí tenemos algunas estadísticas del equipo, si ustedes están interesados pueden ingresar en la página, donde pueden obtener información sobre la mayor parte de los incidentes que se han resuelto en el sistema de diferentes sitios.

Ahora voy a contar algo respecto de los incidentes que hemos resuelto en el pasado.

Un ejemplo de ello es uno muy nuevo que identificó el equipo de CSIRT.CZ en junio de 2012 y que era una amplificación de DNS.

El segundo es un poco más antiguo y tenía que ver con “phishing” y fue resuelto por “cz nic” en otro momento.

Tenemos entonces la amplificación del DNS. Esto fue un ataque a los bancos de Letonia. Hubo muchísimas aperturas del servidor del DNS en todo el mundo. Muchas provenientes de los Estados Unidos, 172 de la República Checa.

Nuestro equipo resolvió este problema con datos relevantes. Los clasificamos y encontramos información sobre los administradores y los contactamos y les pedimos que corrigieran el error.

Esto nos llevó algunos días, pero para nosotros es todavía un proceso constante y sólido, porque teníamos que contactar a los administradores para que resolvieran nuestro problema.

Hoy parece que el 50% del DNS está arreglado.

Hubo muchos nombres de servidores involucrados en este ataque y esto se comunicó el año pasado para el caso de los puertos estáticos.

Investigamos y descubrimos que algunos de ellos, cuatro, cinco o seis, estaban en ambas listas.

También tenemos ataques relacionados con el "phishing". Este problema fue presentado por uno de nuestros registradores. Había registros con diferentes nombres o nombres de dominio, no diferentes, pero todos estaban pagados por una tarjeta de crédito que había sido robada.

Entonces nosotros realizamos la investigación pertinente y descubrimos que el problema tenía que ver con un "troyano".

Este "troyano" atacaba a parte del sistema de ingresos internos de una organización gubernamental de Estados Unidos y esto por supuesto no se podía tratar si no se trataba si no se solucionaban algunas cuestiones previas referidas a la solicitud impositiva.

Durante los siguientes cinco días registramos 150 dominios que tenía este "troyano".

Entonces nuestro equipo pudo desactivar todos estos nombres de dominios y puedo decir que lo hicimos muy rápidamente. Muchos

fueron reactivados una hora después de la registración. Lo cual es un período de tiempo muy bueno.

Esto se llevó a cabo durante cinco días hasta que se solucionó el problema con el registro, con lo cual podemos decir que fuimos exitosos.

Pero hemos discutido este problema y decidimos que no es suficiente estar preparado para un incidente sino que tenemos que ser más proactivos y tratar de identificar los problemas antes de que se transformen en un incidente.

También tenemos nuestro laboratorio donde desarrollamos software especial que se denominaría "gestores de software maliciosos". Tomamos en cuenta ciertos recursos y aquí se acumula cierto dato para luchar contra el "phishing" y entre los datos de fuentes públicas que obtuvimos al respecto, encontramos el de Phishtank, Zeus Tracker, etc.

También hemos elegido sitios y recursos dentro del dominio "cz" y hemos buscados datos de contactos para estos dominios.

Y dado que nuestra solicitud está conectada con un sistema de ticket podemos comunicarnos con los administradores y verificar si pudieron solucionar el problema.

Comenzamos la solicitud en junio pasado, tenemos un año de antigüedad y aquí hay algunos resultados a compartir con ustedes.

Durante un año estamos muy orgullosos de anunciar que tenemos más de 11649 páginas en 2299 dominios, en este gráfico pueden ver información sobre "phishing"; hay porcentaje mostrado sobre las páginas que sufrieron "phishing" a partir de diciembre de 2011. Y

pueden ver que hay una gran caída en junio hacia final del año, en diciembre.

Este gráfico no continúa porque esto muestra el porcentaje en el país.

Estoy seguro de que esto no fue solamente debido al gestor de nombre de dominio malicioso, sino que esto contribuyó a ello.

La solicitud es de fuente abierta y se puede descargar.

Gracias por su atención.

Ondrej Filip: Gracias Martín. Ahora vamos a tener una presentación del registro de los ccTLDs. No vamos a recibir preguntas directamente, luego de la presentación, le voy a dar la palabra a nuestro siguiente orador. Y no voy a leer su biografía porque me va a llevar mucho tiempo y nos vamos a quedar sin tiempo para la próxima presentación.

Pero voy a decir que es una persona que tiene mucha experiencia en procesos de ciber-delito y tiene mucha experiencia a nivel nacional en Serbia y a nivel europeo.

Branko Stamenkovic: Gracias señor Presidente. Como dijo el orador anterior, soy Branko Stamenkovic. Soy Presidente de la Oficina especial, la Oficina de Fiscales Especial de ciber-delito en Serbia, soy parte del Gobierno también, del Poder Judicial del Gobierno.

Y esta es la primera vez que participo en una reunión de ICANN, por lo cual tengo que agradecer a la gente de la ICANN y espero que sean

benevolentes conmigo porque en este momento tengo que dividir mi presentación en tres niveles. Voy a hablar de lo que sucede en mi país a nivel local, a nivel mundial y en la tercera parte voy a contar algunos de los casos que hemos encontrado en Serbia.

A nivel global tenemos varios ataques a nivel de delito cibernético y los hemos tratado.

Tenemos una herramienta, esto se trató en una Convención denominada Convención de Budapest que fue firmada y estuvo abierta en el 2001. Había aproximadamente unos 47 Estados de todo el mundo que fueron signatarios de esta Convención y también la ratificaron.

Lo interesante de esta Convención es que pertenece al Consejo Europeo y es una organización de los Estados europeos, pero está abierta para todos los países de todo el mundo.

Como verán Serbia ratificó la Convención en el 2005, la firmó en el 2005 y la ratificó en el 2009, y la puso en vigencia en agosto de 2009. Los Estados Unidos la firmó en el 2011, la ratificó en el 2006 y la implementación en el 2007.

Esta herramienta les permite a las autoridades de Estado Unidos y a otras unir fuerzas para luchar contra el ciber delito todo el mundo. Esta es la primera Convención y el primer tratado sobre el ciber delito, que va en contra de los incumplimientos y violaciones de los derechos de autor y el fraude y la pornografía infantil y otros tipos de violaciones sobre la seguridad de las redes.

Verán en la pantalla que hay una conducta delictiva en el ciber espacio y esto se divide en cuatro grupos.

Primero tenemos los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas.

Luego tenemos – esto incluye – lo segundo tiene que ver con los delitos relacionados con la informática y el fraude.

Los otros son delitos relacionados con la pornografía infantil y el cuarto son delitos relacionados con los derechos de propiedad intelectual.

En cuanto a la confidencialidad, la integridad y disponibilidad de los datos informáticos y los delitos relacionados tenemos que mencionar el acceso ilegal a los sistemas informáticos, la intercepción ilegal entre otros.

En el alcance de la Convención de Budapest tenemos una conducta criminalista. Hablamos del acceso integral, la intersección ilegal, la interferencia de datos, la interferencia de sistemas, el mal uso de los dispositivos, el fraude, la pornografía infantil y otros delitos relacionados con el IPR.

Y en cuanto a los procesos hablamos de la preservación sumaria, la búsqueda y la suspensión y la intercepción de los datos informáticos.

Esto tiene un marco legal del país, aunque las herramientas se utilizan en el sistema legal.

Finalmente, esto hace que todas las autoridades sobre delitos referidas al ciber delito en el mundo estén en la misma página respecto de las herramientas que utilizan para luchar contra el ciber delito.

A nivel local tenemos un ejemplo de Serbia que comienza allá por los ’90, una de las más importantes actividades o tareas que tenemos por hacer tiene que ver o está a nivel nacional.

Afortunadamente el Ministro de la Agenda Digital y la República de Serbia han adoptado la estrategia nacional para toda la sociedad de la información que es clave. Es un documento clave en realidad que explica la protección de internet y el ciber espacio referido a Serbia. Esto es a nivel nacional.

Podemos ver entonces que hay una estrategia nacional para el desarrollo y la confianza de los ciudadanos y es una función de seguridad; también tenemos la necesidad de utilizar la información y de tomar medidas de seguridad al respecto, entre otras cosas.

Lo específico de mi país es que en una etapa muy temprana comprendimos la necesidad de tener una autoridad gubernamental especializada para combatir el ciber delito. Y en este momento incluso en la actualidad de la Unión Europea este tipo de especialización es más bien rara.

Una de las razones por las cuales esta especialización no surgió en mi país es la siguiente. Tiene que ver con la carga y con el alcance del ciber delito que era muy alta a fines de los ’90 y a principios del 2000. Había una gran ignorancia respecto de los procesos normales y mi país tenía que tener una autoridad especializada para poder tratar este nuevo desafío, esta nueva amenaza que era el ciber delito que afectaba a Serbia y también al mundo desde Serbia en adelante.

Como pueden ver, la idea surgió en los ’90, luego se mejoró en el 2004, se propuso un borrador de la ley que propuso la Asamblea General en el 2005. Le ley fue adoptada por la Asamblea Nacional y desde el 2005 en adelante hasta la actualidad tenemos una ley especial sobre la organización y competencia de ciertas autoridades gubernamentales para luchar contra el ciber delito en Serbia.

Esta ley incluye la organización, es una ley de procedimientos, una ley organizativa, no es una ley sustancial, pero incluye la organización entre tres niveles y autoridades gubernamentales.

Tenemos un servicio especial dentro del Ministerio del Interior, luego tenemos una Oficina de Fiscal especial y también un Tribunal especial para tratar los ciber delitos.

Ahora estamos al comienzo de lo que podemos llamar – o estamos formando es SIRTs nacional y próximamente este organismo va a ser creado y va a brindar protección también.

Brevemente quiero repasar la legislación sustancial. Tenemos distintos grupos de delitos dependiendo de la manera que son llevados a cabo y cómo los delincuentes actúan al momento de cometer estos delitos.

Debo decir que todos estos actos criminales están dentro del marco de esta Convención.

Como les dije, tenemos una guía especial. También tenemos un servicio especial para delitos cibernéticos y luego tenemos una organización y la competencia de los distintos tribunales. Tenemos el alto Tribunal de Belgrado que se encarga de estos casos. Vemos los datos estadísticos

para la Fiscalía pública especial, respecto de los ciber delitos. Tenemos más de 2600 casos en este momento.

Quiero decir algo respecto de los casos. Y si, ahí vemos una máscara en pantalla, la famosa máscara; estos casos son nuevos, este es el primer caso en el cual nos encontramos con la organización "Anonimus" en Serbia que nos llamó la atención porque intentaba entrar en profundidad en algunos de los servidores del Gobierno.

Ellos trabajaron en los servidores del Ministerio de Justicia de la Fiscalía pública y en otros servidores públicos también. Teníamos falsos DNS y utilizaban también representación o anonimato para poder llegar a estos sistemas. En última instancia lo que hicimos fue lo siguiente. Nos dimos cuenta de que en los últimos seis meses este delincuente pudo tener más de 756 mil puntos de PHP diseminados en todo el mundo y en Serbia.

Es decir que una sola persona tuvo éxito y pudo penetrar en ese momento en el 50% de los proveedores de servicios de internet serbios y tomó el control de los servidores de ruteo de esos ISP y también controlaba los datos de esos principales proveedores de servicios de ISP.

Una de las principales amenazas tiene que ver con el abuso de tarjetas de créditos, obviamente que siempre provienen de parte del uso de identidades probadas o identidades falsas en internet y deriva del uso de tarjetas de créditos con Proxy o representaciones de titularidad anónimas.

Al final de la implementación o ejecución de estos delitos siempre descubrimos que hay un ciudadano, pero vemos que la mayoría de los ciudadanos sufren la falta o la sustracción de sus bienes o de su

propiedad a través del uso indebido de sus tarjetas de créditos. Entonces estos delitos ponen en peligro a una persona común y corriente.

Uno de los casos con los cuales trabajamos tiene que ver con la pornografía infantil en internet, por definición siempre los delincuentes que cometen estos delitos utilizan falsos DNS, utilizan Proxy anónimos, utilizan servidores que están por debajo de la red. Es decir, todo tipo de espacio que los proveedores, o el Gobierno, o los proveedores de servicios de internet no pueden controlar.

Entonces, cuando buscamos a esos delincuentes tenemos que armarnos de mucha paciencia, mucho conocimiento y mucha cooperación internacional.

En algunos momentos encontramos que no tenemos tanta cooperación por parte de las autoridades o de los ISP extranjeros, pero debo reconocer que hemos tenido muy buena cooperación con las autoridades estadounidenses respecto de estas problemáticas y también debo decir que el peligro de la pornografía infantil en internet que está presente en todo el mundo va a ser que se despierten todos los que aún están dormidos respecto de este tema.

También aquí vemos otro caso interesante acerca del abuso del dominio de internet, en este caso se usó un falso DNS “europe.com” en inglés, esto fue utilizado por delincuentes de Serbia que básicamente solicitaban realizar una custodia de datos, datos en línea, pertenecientes a los Estados Unidos y luego lo que hacían era vender o comercializar artículos antiguos, o antigüedades; se veía que algunos de los artículos que ellos adquirían mediante estos delitos en internet, bueno, vemos que eran artículos muy caros que valían miles de dólares y vemos que

como resultado de esta acción pudimos confiscar o recuperar algunos de estos objetos.

Esto es un panorama interesante de lo que los delincuentes que cometen este tipo de delitos están listos a realizar para poder obtener un rédito económico. Por ejemplo van a transferir, este artículo que vemos aquí en pantalla, de Oregón a Belgrado, utilizando carga aérea. Y luego también vemos todos los ataques al DNS que son muy frecuentes y que pueden causar un daño muy grave, no solamente a los proveedores de servicios de internet sino también a sus usuarios, es decir, las empresas, los negocios, por ejemplo este ataque de DDS, de denegación del servicio, dejó sin acceso a gran parte de Serbia, sin acceso a internet durante doce horas. Entonces la columna vertebral de comunicación entre los proveedores de Serbia y los proveedores fuera de Serbia se vio en peligro y no pudimos tener tráfico entrante ni saliente en Serbia

Entonces, en resumen, si, soy miembro del Gobierno, soy parte del sistema judicial, penal, ustedes vieron en mi presentación que las autoridades gubernamentales hoy en día tienden a especializarse y van a ver que hay funcionarios, policiales, organismos encargados del cumplimiento de la ley que son cada vez más especializados. Va a ver fiscales mucho más especializados, jueces mucho más especializados, quienes serán los encargados de solicitar mayor información, de enviar notificaciones, citaciones y que trabajarán realizando una labor transfronteriza porque el delito cibernético es un delito transfronterizo.

Utilizaremos nuestras herramientas a nuestro alcance, como por ejemplo la Convención de Budapest para solicitar pruebas, para solicitar

información y lo haremos en cooperación con nuestros colegas de las otras fiscalías, de los demás organismos de cumplimiento de la ley. Y esto se trata de proteger no sólo nuestra sociedad sino de las sociedades de todo el mundo.

Muchas gracias por su atención.

Ondrej Filip: Gracias Branco por su presentación. Vamos a hablar ahora acerca de las capturas de los nombres de dominios. Y vamos a focalizarnos entonces en la presentación de Christopher Malone, que está sentado aquí y será quien comience con su presentación.

Christopher Malone: Gracias señor Presidente. Gracias Martin, Como se dijo, yo soy Christopher Malone. Soy un agente especial del Departamento de investigaciones de seguridad internet. Trabajo en la ciudad de Washington en lo que llamamos C3.

Mi colega y yo somos miembros del grupo asesor ad-hoc en el GAC en temas de cumplimiento de la ley.

Ustedes sabrán que nosotros participamos en ese organismo o en ese órgano, en cuestiones que tienen que ver con seguridad pública, no solamente con el cumplimiento de la ley en lo que respecta a preocupaciones relacionadas con la transición al IPv6, con la retención de registros estandarizados, los períodos respectivos, la exactitud de esos registros. Pero vamos a hablar acerca de la exactitud y de la importancia de los datos de WHOIS para nuestra tarea.

Nosotros en debates con integrantes de la DEA, del Servicio Secreto, del FBI y con nuestros colegas extranjeros de por ejemplo de SOCA y del Reino Unido, de RCM, todos compartimos la misma postura con respecto a la exactitud de los datos del WHOIS y a su importancia para nuestra tarea.

Al interactuar con ellos debatimos frecuentemente este tema y damos por sentado que la gente entiende que nosotros realizamos investigaciones y que para nosotros entonces esto es importante. Quizás para los otros esto sea obvio, probablemente haya personas que no conocen las metodologías que utilizamos para hacer nuestras investigaciones.

Habiendo dicho esto, tengo una breve presentación, pero que parecería ser una manera mundana en la cual hacemos estas investigaciones pero quiero darles una perspectiva de importancia de estos datos y de su exactitud para poder iniciar parte de nuestras actividades.

Hoy me pronuncio a favor de los investigadores, los investigadores que trabajan en el campo haciendo sus investigaciones penales, en contraposición a un punto de vista político, o tampoco un punto de vista desde el punto de vista del Gobierno o de política pública. Sin bien defendemos también un buen gobierno y una buena política pública.

Entonces vamos a hablar acerca del valor de la exactitud de estos datos.

Un agente en nuestra organización tiene direcciones de IP a través de diferentes medios, probablemente pueda ser solicitudes de direcciones de IP, a través de contenidos de internet. También puede estar asociada

esta dirección de IP, asociada a diferentes correos electrónicos, relacionados con actividad delictiva.

Para nosotros esta es información de un IP sucio. En nuestra jerga. Entonces, la respuesta inicial es ir o recurrir a estos recursos d código abierto para rastrear al titular de ese registro a un proveedor de servicios de internet que nos pueda indicar quién es el suscriptor y poder identificar entonces a ese delincuente.

Entonces recurrimos al WHOIS, al sitio web de ARIN, es decir, todas las herramientas de código abierto para poder conectarnos con ese proveedor de servicios de internet.

Luego el agente va a generar una citación a través de distintos procesos legales, en mi país se va a realizar una investigación a cargo de "El gran jurado" y luego vamos a tratar de tener información adicional de ese suscriptor, para ver dónde está ese potencial delincuente.

Es importante que les diga que estas herramientas o autoridades ya están en funcionamiento y que mis colegas, en la mayoría de los casos, tienen herramientas o autoridades similares. Pero, lo que estamos debatiendo aquí no es una expansión de estos procesos jurídicos que están bajo escrutinio en los Estados Unidos, sino que en última instancia en algún punto al final de un proceso de investigación, siempre habrá un fiscal, un juez y también en algunos casos un jurado integrado por doce miembros.

Entonces, esto no es una investigación única, y tampoco queremos expandir o ampliar estas herramientas. Sino que más bien, este paso

inicial para la gente que está haciendo su investigación de campo es esencial, es esencial poder tener estos registros exactos.

Cuando se genera esta citación obviamente el proveedor de servicios tiene un período, un plazo para responder que generalmente se le da de 14 a 30 días. Al final de ese plazo como ustedes se imaginan, si el proveedor de servicios de internet no responde le enviamos una nueva solicitud debido a la ausencia de su respuesta.

Entonces, como se imaginarán, cuantos más obstáculos enfrentemos, más tiempo llevará la investigación.

Como ustedes saben estos datos cibernéticos son datos perecederos o no duraderos, entonces tenemos legislación, por ejemplo en mi país – que regulan esta situación. Pero cualquier tipo de retraso en la obtención de esta información obviamente retrasa a la investigación en sí misma.

También quiero hacer referencia a otras técnicas de investigación.

La obtención mediante un proceso jurídico apropiado de la información de un suscriptor no nos lleva inmediatamente al delincuente al cual estamos apuntando. Sino más bien que nos lleva a otra investigación que requiere el uso de todas las otras herramientas en la investigación.

El investigador tiene que investigar a la persona que está pagando esas cuentas o esas facturas y probablemente esa persona no sea el potencial delincuente. Sino más bien que la investigación previa realizada por el investigador posibilitará la identificación de ese individuo mediante evidencias digitales y otras evidencias que harán un exitoso trabajo después de la Fiscalía.

A menudo, para nosotros estos es un emprendimiento que implica utilizar muchas bases de datos, pero a veces esto no nos lleva a ninguna parte o bien nos lleva a una búsqueda adicional.

Esta es una de las cosas que quería aclarar para darles una perspectiva. Generalmente vemos que los recursos de los gobiernos deben ser ilimitados. Y hablo en defensa de ese agente que trabaja en el campo con cinco o diez, veinte casos a la vez, que tienen que revisar estas investigaciones y que tienen que lidiar por ejemplo con la posible explotación o el abuso infantil en internet. Y esos períodos extensos que permiten la respuesta de los proveedores de servicios de internet hacen que sea necesario que los datos de WHOIS que nos dan sean exactos.

Habiendo dicho esto, le cedo la palabra a mi colega.

Christopher Landi: Buenas tardes o buenas noches a todos. Soy Christopher Landi. Trabajo con el Centro de investigación de delito cibernético de la unidad de seguridad interna en mi país.

Quiero hablar con ustedes acerca de lo que sucede cuando identificamos el abuso de un dominio.

Ya sea un dominio donde hay imágenes de pornografía infantil o un dominio que está en violación de derecho de propiedad intelectual.

Una de las herramientas que podemos utilizar para quitar las imágenes de internet, es justamente recurrir a la captura del nombre de dominio. Es algo que a lo mejor suena un poco que parece intimidatorio, pero nosotros nos lo tomamos muy en serio.

Nosotros implementamos estas capturas de nombres de dominio para justamente capturar a las personas que están haciendo daño. Por ejemplo las personas que publican imágenes de abuso infantil, es decir, vamos detrás de esas personas. Uno de los primeros pasos que hacemos es identificar la URL, nos aseguramos que todos los caracteres, que toda la tipografía coincida exactamente. Porque si uno comete un error de tipeo comete un error.

Y el resultado es distinto.

Luego queremos saber exactamente dónde está albergado ese contenido ilícito, puede estar al tercer nivel, en una sub-carpeta. Es decir, dónde está. Si está en una sub-carpeta queremos ver dónde está guardado dentro de esa sub-carpeta.

Luego, vamos a verificar el contenido. Podemos obtener información de la URL por parte de un organismo de cumplimiento de la ley, de uno de los titulares de los registros, de un ciudadano individual. Verificamos el contenido. ¿Es realmente contenido de abuso infantil? ¿Está todavía ahí ese contenido? Entonces luego, capturamos los contenidos del sitio web para poder saber qué es lo que estaba allí exactamente en el momento en que capturamos ese contenido.

Luego identificamos al registratario de ese sitio web. Porque es muy importante saber quién es el dueño de ese sitio web para la investigación.

Eso puede retrasar la investigación. En algunos casos significa que las víctimas infantiles están siendo mostradas en línea en internet y hay imágenes o grabaciones en vivo de estos casos de abuso infantil.

Una vez que hemos identificado eso, identificamos a quien está haciendo el servicio de "host" o quien está albergando a la URL, luego vemos si hay contenido legítimo que ha sido el caso en algunas oportunidades.

Supongamos que si es un material antiguo de explotación o abuso infantil, lo que vamos a hacer es, mediante un proceso legal lograr que se cierre ese sitio web.

Probablemente notifiquemos al titular de ese registro de que hay contenido ilícito, pero siempre vamos a recurrir al proceso jurídico, judicial correspondiente para lograr el cierre del sitio web.

Esto tiene que ver también con los distintos sitios o ubicaciones donde está albergado este sitio web.

Pero quiero que todo el mundo entienda que no vamos detrás de sitios web de personas que tienen una imagen protegida por Copywrite en su sitio web. Sino de personas que ganan millones o miles de millones de dólares teniendo ciento de miles de imágenes o los fabricantes o distribuidores o productores de pornografía infantil.

Esas son las páginas web que queremos cerrar.

Y habiendo dicho esto, le cedo la palabra a Ondrej.

Ondrej Filip: Gracias por la presentación. Ahora es el momento donde ustedes, damas y caballeros, pueden hacer preguntas.

¿Hay alguna pregunta? Por favor diga su nombre y asociación.

Frank Schilling: Soy Frank Schilling y soy un solicitante de registro. Y espero ser un operador de registro.

Viene para la siguiente sesión en realidad. Pero su sesión ha sido muy interesante. Como consumidor de internet, y como registrador y futuro operador de registro, quiero decir que hay un riesgo para todos o hubo un riesgo a partir del 11 de setiembre. El Gobierno tendía a protegernos pero el riesgo que corremos a partir de esa fecha es que estamos cometiendo errores todo el tiempo. Y llegamos a un lugar donde parece que es poco solucionable.

Ustedes hacen un gran esfuerzo y su esfuerzo es respetable, porque nadie de nosotros quiere ver pornografía infantil claramente. Nadie quiere que se violen las leyes y conforme uno se transforma en un juez o un jurado o en un ejecutor de este movimiento, por así decirlo, aparecen otras figuras que tenemos que tener en cuenta y esto de alguna manera nos crea nerviosismo.

¿Podrían ustedes hablar o contarnos si tienen alguna especie de discusión interna? En lugar de hablar de errores o de los incidentes que tienen. ¿Tienen alguna especie de control interno implementado?

Por ejemplo ¿Cuáles son las medidas que se toman? Es decir ¿Cuáles son las distintas acciones que tienen para sus diferentes acciones?

No sé si me están entendiendo con esa pregunta.

Christopher Landi: Seguramente voy a responder a esa pregunta. Hay ciertas verificaciones que se hacen. Yo mismo no puedo dar de baja a un dominio. Hay ciertos niveles a tener en cuenta.

Hay múltiples agencias, hay supervisores del Gobierno, hay un primer nivel y un segundo nivel de supervisión donde intervienen los Fiscales, donde intervienen los letrados patrocinadores.

Entiendo lo que usted me dice, entiendo su pregunta respecto de si hay algún control. Pero para responder a su pregunta lo que le puedo decir es la razón por la cual las agencias de cumplimiento de la ley vienen a estas reuniones. Es porque nosotros cuidamos o vemos a la comunidad. Y tenemos un montón de respuestas para darles a la comunidad.

Nosotros estamos aquí para decir “estos son los temas”. Estas son las cosas que estamos solucionando. Estos son los asuntos técnicos con lo que estamos lidiando. ¿Cómo los resolvemos? ¿Cómo permitimos que internet continúe siendo libre como lo es sin tener estos malos actores que están ahí arruinándolo todo?

Desafortunadamente ¿Cuántos niños son abusados gracias a ellos?

Frank Schilling: Creo que nadie tiene una buena respuesta para eso claramente.

Pero tenemos que saber que tiene que haber cumplimiento de la ley y usted habló mucho acerca de las verificaciones y las supervisiones. Entonces tenemos que tenerlas en cuenta y ver hasta dónde vamos a llegar.

Si tenemos que seguir avanzando si sabemos que nos vamos a mover en un ambiente que no es sano.

Y yo por ejemplo soy estadounidense, yo vivo en Estados Unidos, me encanta mi país, veo la televisión de mi país, pero creo que hay un riesgo cuando vamos a cierto tipo de discusiones y esto nos lleva a una discusión lógica. Y quizás a veces nos alejamos del objetivo.

Y esto es algo que a veces me quita el sueño. Cuando las cosas no están bien. Por eso pregunto si tienen controles internos o por eso ustedes asisten a estas reuniones.

Christophre Malone: Perdón. Simplemente para amplificar la discusión. Los investigadores criminales o de delitos hacen verificaciones y tienen los instrumentos necesarios para implementarlos. Por ejemplo, un Fiscal sería un organismo o un control.

Es decir, el último árbitro es el jurado en sí mismo, pero también hay otros puntos para tener en cuenta.

Hay una nebulosa en las actividades de inteligencia que tienen que ser supervisadas. Y tenemos también herramientas judiciales y una serie de niveles donde tenemos que actuar y donde tenemos investigadores.

Y francamente hay que tener el tiempo para hacer esto.

Tenemos redes de actividades y esto es de la manera que llevamos a cabo nuestros controles internos cuando llevamos a cabo una investigación.

Nancy Lupiano: Perdón. Estamos llegando al final de la sesión. Cinco minutos como mucho.

Elliot Noss: Soy Elliot Noss y quisiera hablar un poco sobre el conocimiento o sobre lo que usted mencionó respecto de la pornografía infantil.

Conté que usted hizo referencia varias veces a los temas de propiedad intelectual. Y también habló de las personas que ganan miles de millones de dólares al respecto.

La razón por la cual yo digo esto es que hay datos públicos que están disponibles y la mayoría de estos captores de nombres de dominio tienen que ver o encuentran información sobre la propiedad intelectual. Y este tema de la propiedad intelectual ha propiciado la expansión del crimen en los últimos cuatro o cinco años en los Estados Unidos.

Entonces, cuando hablamos de estos temas creo que es más creíble, porque no creo que haya nadie en esta sala que esté a favor de la pornografía infantil, hablar de otros temas que son más controversiales, como por ejemplo la expansión y la penalización de los derechos de propiedad intelectual.

Es decir, hubo un caso de traición de un joven de 22 años en el Reino Unido y donde ahora solamente tenemos una expansión de la criminalización de ellos en un país.

Esto es algo interesante y estas cuestiones no afectan sólo a la comunidad de ICANN sino a la comunidad mundial.

Y yo sugiero esto, porque nos vamos a alinear mano a mano cuando hablemos de la pornografía infantil. Pero hay otros delitos que tienen que ver con los nombres de dominios que van más allá, que tienen una expansión que abarcan o afectan mucho más a los derechos. Entonces tendríamos que de alguna manera separarlos, aislarlos en forma claramente para identificarlo como cuestiones criminales o delictivas.

Sé que hay una significativa cantidad de la comunidad que ve necesario el tratar el tema de los derechos comerciales privados y su violación.

Christopher Landi: Aprecio su comentario y creo que el IPR es una cuestión más bien legislativa. No puedo hablar a mi agencia y ver si yo estoy de acuerdo o no.

Pero puedo decir que si hay delitos financieros que cuestan miles de millones de dólares.

¿Y está esto relacionado con el IPR?

En algunos casos si, están relacionados con violaciones al IPR, pero en otros casos no.

Entonces. Nosotros investigamos este tipo de delitos, en cuanto al IPR, es fácil, quizás la explotación infantil es lo más sencillo de los dos. Porque es un tema que está investigado a nivel político y público. Pero hay otra serie de leyes que se deben modificar o implementar.

Quizás hay gente que hace lobby para permitir el abuso de un niño de dos años, entonces, todos estamos en contra de eso, no hay nadie que esté a favor.

Pero en cuanto a las violaciones del IPR yo entiendo lo que usted dice y entiendo el conflicto que presenta.

Zahid Jamil: Gracias. Ondrej tiene la palabra.

Oondrej Filip: Gracias.

Zahid Jamil: Quisiera hacer un comentario respecto del IPR.

Hablo en representación propia. Vengo de una parte del mundo donde el IPR, se ve como un organismo que alimenta al delito. Entonces, hablando de los proyectos que se tienen en cuenta.

Me parece a mí que todavía no se ha logrado el nivel de cumplimiento necesario respecto de internet. Y entonces pienso lo que dijo Branko respecto del ciber delito y hasta qué punto ve usted en esto como una forma global. Porque me parece que yo no sé que la Comunidad europea, Canadá, Estados Unidos o Japón tengan a esto como algo extraño.

¿Cómo ven ustedes a la Convención global?

En cuanto a las agencias de cumplimiento de la ley internacional, creo que tienen que tener acceso a estas cuestiones.

Y otra cosa. ¿Podemos tener copias de esta presentación? Porque no se encuentran en el sitio actualmente.

Margie Milam: Si van a estar publicadas en la página.

Branko Stamenkovic: Si, veo que la Convención de ciber delito como herramienta global ha sido respaldada, digamos por varios miembros del Consejo de Europa y los Estados Unidos y Japón, también la ratificó, hace algunas semanas. La ratificó en la última conferencia de octubre, hace algunas semanas también el Consejo de Europa reconoció a muchos países de América del Sur y del lejano Oriente.

Así que están listos para implementar esta Convención de ciber delitos y si no, no están listos para implementarlas están listos para ratificarla. Y han también implementado las disposiciones de la Convención de Budapest para implementar herramientas legales a fin de luchar contra el ciber delito y nos gustaría ver también que cada vez más países estén dentro de este proceso establecido por la Convención.

Ondrej Filip: Me temo que tenemos que finalizar aquí, les agradezco a todos los panelistas por sus disertaciones. Ha sido una sesión muy interesante.

Gracias. Fin de la transcripción -