SAN JUAN – Cómo funciona: entendiendo el abuso del DNS
Lunes, 12 de marzo de 2018 – 13:30 a 15:00 AST
ICANN61 | San Juan, Puerto Rico

ORADOR NO IDENTIFICADO: Buenas tardes. ICANN61. 12 de marzo. Cómo Funciona: Entendiendo el Abuso del DNS.

CATHY PETERSEN: En breve vamos a iniciar la sesión sobre cómo funciona y cómo entender el abuso del DNS.

Buenas tardes a todos. Vamos a ver esta sesión de cómo funciona: Cómo entender el abuso del DNS. Tenemos a Carlos Álvarez de la oficina del Director Técnico, que va a presentar esta sesión.

CARLOS ÁLVAREZ: Gracias, Cathy. Gracias a todos. Sé que hay unos 23 participantes en línea, así que vamos a iniciar la sesión.

Vamos a hablar entonces de un tema que es muy importante. Realmente es pertinente. También es conflictivo en algunos aspectos y creo que todos tienen que prestar atención a esto, porque vamos a hablar del abuso en el DNS.

Nota: El contenido de este documento es producto resultante de la transcripción de un archivo de audio a un archivo de texto. Si bien la transcripción es fiel al audio en su mayor proporción, en algunos casos puede hallarse incompleta o inexacta por falta de fidelidad del audio, como también puede haber sido corregida gramaticalmente para mejorar la calidad y comprensión del texto. Esta transcripción es proporcionada como material adicional al archive, pero no debe ser considerada como registro autoritativo.

En primer lugar, vamos a establecer de qué vamos a hablar exactamente, porque hay distintas formas de entender lo que es el abuso de DNS y hay distintas perspectivas. Vamos a hablar de cuáles son esas perspectivas. Después vamos a ver algunos ejemplos de lo que es el abuso o el uso indebido del DNS. Después vamos a hablar de cómo ha evolucionado todo este panorama en cuanto a las amenazas del DNS y después vamos a finalizar hablando del abuso del DNS dentro del contexto de la ICANN.

Lo primero que se ha de mencionar es que no existe una definición aceptada internacionalmente de qué es el abuso del DNS. Como dice acá esta imagen, hay distintas variantes de la definición. Algunos incluyen el delito cibernético, otros hablan del *hackeo* y otros de una conducta maliciosa.

Entonces las amenazas al DNS también pueden ser corrupción de datos, denegación del servicio y privacidad. Y también se hace una diferencia entre lo que es el abuso del DNS y el uso indebido del DNS. Lo que dice la transparencia es que el uso indebido hace referencia a actividades no solicitadas que pueden ser conspirativas y que hacen un uso activo del DNS o los procedimientos para registrar o resolver nombres de dominio. Después vamos a ver exactamente de qué se trata. Y esto lo vamos a ver después también.

Lo que dijo el GAC tratando de llegar a una definición o dar elementos para entender qué era el abuso del DNS, ¿qué es lo que dijo el GAC en relación entonces con esta área tan amplia? El GAC en su comunicado brindó medidas de protección aplicables a todos los nuevos gTLDs y un extracto de este documento que habla de mitigación de la actividad abusiva habla de cierta actividad abusiva como distribución de software malicioso, operación de *botnets*, *phishing*, piratería, violación a los derechos de autor y marcas comerciales, prácticas fraudulentas o engañosas, falsificación o que de otro modo significan una actividad contraria a la aplicación de la ley.

Esto es algo muy amplio, y algunos piensan que algunos de los temas incluidos acá no representan un abuso técnico del DNS en cuanto a protocolos técnicos o el sistema. Pero, como dije, estas son distintas visiones que tiene la comunidad. Y esta es una de las visiones que tiene la comunidad, sobre todo cuando habla de violación de derechos de autor y marcas comerciales, a veces, o prácticas fraudulentas o engañosas, no se consideran técnicamente abuso del DNS.

Hay una gran pregunta –la voy a dejar abierta durante la sesión—que tiene que ver con si el *spam* es o debería ser considerado un abuso del DNS, del sistema de nombres de dominio.

Del lado de los organismos de aplicación de la ley, de la comunidad técnica, el *spam* es un predecesor de otros tipos de actividades maliciosas, pero en sí mismo, al menos hasta el día de hoy, no ha sido considerado un abuso técnico del DNS global, del sistema de nombres de dominio global.

Cuando están haciendo entonces la investigación sobre amenazas y analizan los datos, ustedes pueden ver que hay una campaña de *spam* que fue lanzada como para saber cuál es la infraestructura e identificar la infraestructura criminal que están utilizando estos actores para esta campaña. Y si siguen con la actividad, finalmente van a ver que hay otras actividades vinculadas que siguen después de esta actividad. Puede ser distribución de material abusivo, *phishing*, distintos tipos de cosas. Para decirlo en términos simples, el abuso del DNS hace referencia a cualquier cosa que ataque o abuse de la infraestructura del DNS. Después lo vamos a ver más en detalles.

Hay muchas formas en las que podemos ver el abuso del DNS. Podemos hablar de dos formas de abordar este tema. Una es la perspectiva del abuso de la resolución de los nombres de dominio, que es la parte técnica de cómo los nombres de dominio se traducen en direcciones IP. Y la otra perspectiva de la que vamos a hablar tiene que ver con la registración de los nombres de dominio.

Estos son servicios que brindan los registros y los registradores, y entonces hay un abuso por parte de los delincuentes de diferentes formas. Y vamos a hablar de esto también.

El uso indebido del DNS hace referencia entonces a explotar el protocolo de DNS o los procesos de registración de nombres de dominio con fines maliciosos. Esto está ejemplificado y explicado con mayores detalles más adelante. Acá estoy donde quería.

No necesitan leer todo lo que dicen las transparencias, porque lo que quiero mostrarles acá es cuáles son los elementos operativos del DNS en escala simplificada.

Tenemos arriba en azul lo que son los servidores de nombres de dominio autoritativos, que son los que tienen los datos, son autoritativos para el nombre de dominio para cada TLD. Por debajo tenemos resolutores recursivos, que los pueden ver como los servidores del DNS, que el ISP que ustedes tienen que es el que les brinda el acceso a Internet, les permite utilizar. Da un servicio de resolución de DNS.

Después tenemos lo que son los resolutores terminales o clientes. Estos resolutores terminales *stub* son estos. Es una función dentro de mi navegador, por ejemplo, que busca la información que necesita para utilizar los recursos que yo quiero utilizar.

Por ejemplo, yo voy al navegador y pongo www.icann.org, entonces este resolutor terminal me va a resolver este nombre de dominio dentro de una dirección IP, y dónde está el contenido de icann.org y me lo va a bajar a mi dispositivo, lo voy a poder ver y voy a poder interactuar con él, etc.

Estos tres elementos operativos del DNS son objetivo de ataques. Bueno, todo es blanco de ataques, ¿no? Vamos a ver ejemplos.

Acá esto se pone interesante entonces. Porque vamos a hablar entonces de la reflexión y la amplificación. Esto tiene que ver con los ataques de DDoS que son los de Denegación de Servicio.

¿Qué es la reflexión? La reflexión significa que podemos enviar un paquete y falsificar la información sobre la dirección IP fuente para que entonces el servidor piense que lo mandó otra persona. Tenemos ese servidor que envía una respuesta a esa otra dirección IP. Entonces si mi objetivo es atacar a Cathy, yo le envío el paquete al servidor del DNS y la dirección IP que voy a incluir en ese paquete va a decir que el paquete viene de Cathy, y no viene de mí.

Si yo uso los resolutores abiertos, que son servidores DNS que existen y hay miles de ellos, que no pueden resolver las consultas de las direcciones de IP y que están resolviendo para otras partes del mundo, entonces Cathy va a tener muchísimos

paquetes porque tenemos todos esos paquetes y esos resolutores que están en todas partes y entonces todos van a pensar que las consultas las envió Cathy y entonces todos le van a responder a ella. Eso es reflexión.

El otro vector se llama amplificación. Amplificación significa que todas esas consultas que yo estoy enviando son pequeñas. Puede ser, y en general se trata de una línea de comando. Esa línea puede ser tan simple como *dig* nombre del servidor, nombre de dominio. Siete *bytes*, nada más. Es poquito nada más. Pero la respuesta va a ser muy grande, pueden ser 2.3, 2.5 o 2.7 megabytes. Hay que multiplicar eso por las miles de consultas que yo estoy haciendo que mi *botnet* envíe. Los *botnets* son grandes redes de algunos dispositivos que pueden manejar cientos de dispositivos comprometidos. Entonces el delincuente que está con el *botnet* va a tener a todos esos dispositivos comprometidos que envían consultas a esos resolutores ahí para que le envíen la respuesta a Cathy.

Hay una multiplicación entonces. Eso tiene que ver con los dispositivos que están comprometidos, que yo recluté, que son parte de mi *botnet*. Por la cantidad entonces de resolutores que yo estoy potenciando y envío el comando, envío esta consulta que les obtiene información de DNS. Esto dispara una respuesta. Y este comando es tal que como dije, la consulta es pequeña pero la respuesta es muy grande.

Entonces Cathy va a tener muchísimas cosas y puede ser infectada si no tiene algún tipo de seguridad. Y además va a colapsar si no tiene forma de hacer frente a todo lo que le está llegando.

Después, en el 2003 se utilizó el DNS como vector de un ataque DDoS contra Spamhaus. Hubo un ataque a esta empresa, que dio buena información sobre lo que era la mitigación y la protección contra amenazas.

Y obviamente los ataques evolucionan. El DNS no es el único vector, sino que es uno de ellos. Pero como protocolo está siendo explotado.

También tenemos lo que es el envenenamiento del caché o el ataque de agotamiento. Y después lo que es el ataque del intermediario del DNS. Después los vamos a ver.

Esto es básicamente lo que yo acabo de describir. Tenemos un ataque que usa la reflexión, porque envía paquetes que están falsificando la dirección IP, entonces todos estos resolutores abiertos piensan que el dispositivo de Cathy es el que está enviando las consultas. La consulta que reciben es tal que dispara una respuesta muy grande. Este es el vector de amplificación. Cathy entonces recibe toda esta cantidad de información, que es lo que yo acabo de describir.

Este no fui yo. A ver. Tomé demasiado café, por eso avancé muy rápido. A ver, estábamos acá. Bien.

Otra forma en la que se puede atacar el DNS es a través de los servidores de nombres de alguien. Estos servidores dan resolución para un nombre de dominio, entonces si yo digo "carlos punto lo que sea", y digo idealmente que tengo que ir a servidores donde el DNS como sistema global, va a obtener información sobre los recursos que yo tengo asociados con ese nombre. En otras palabras, yo voy a definir y voy a poner a disposición esa información a través de estos servidores de nombres y entonces las direcciones de IP donde está mi correo electrónico, donde está el servidor de web, donde está mi FTP, etc.

Entonces si alguien va a ir mis servidores de nombre y lo que quiere falsificar, no va a recibir esa información. Yo no voy a poder recibir correo electrónico, no voy a poder enviar, la gente no va a poder a mi sitio web, etc. Entonces puede haber consecuencias si estamos hablando de un nombre de dominio de valor, no en el caso de "carlos". Pero bueno, podría ser.

Este tipo de ataque hace un abuso delictivo del protocolo TCP. Cuando envío un paquete de TCP al servidor, el servidor me responde. Esto es en términos muy simples. Entonces le responde a la conexión de TCP, tanto el dispositivo que inició la

conexión como el servidor que responde, se dan la mano. Y eso genera un canal de comunicación que mantienen ambos. Es decir, los dos tienen que asignar ciertos recursos para mantener ese canal de comunicación.

Si tengo yo muchos dispositivos comprometidos en un *botnet* y todos envían respuestas y consultas a un servidor de nombre de forma que va a ser que este servidor establezca demasiados apretones de mano TCP, es decir, muchos recursos para mantener estos canales de comunicación establecidos a través del TCP, llega un punto en el que ese servidor ya no va a tener recursos disponibles para asignar ninguna otra conexión de TCP. Es decir, nadie va a poder pedirle información del DNS a ese servidor. Va a seguir estando en línea, pero no va a poder responder a ninguna consulta. Esto es lo que dice acá, porque dice que entonces se degrada o se interrumpe la respuesta.

Si no podemos resolver ese nombre en algunos minutos, imagínense si estamos hablando de mucho tráfico y lo multiplicamos por miles. Cuando hablamos de un nombre dominio quizá pierdan totalmente la resolución del nombre. Y obviamente todos queremos evitar esto porque es el peor de los casos.

El envenenamiento del caché. Esto es tramposo, porque los malos son creativos, como siempre. Bueno, no siempre, pero a

veces son creativos. Recuerden que yo mencioné anteriormente que tenemos servidores de nombres autoritativos, en la parte superior, y que lo asociaba ns1.carlos.loquesea para darle el DNS con la información vinculado con lo que era mi servidor de red, mi servidor de correo, etc. Esos son mis servidores de nombres autoritativos.

Pero después todos los ISPs y todos los que están ahí, 9.9.9.9 o 8.8.8.8, los distintos proveedores de DNS tienen recursivos, es decir, que hacen preguntas en nombre de otros. Algunos de estos resolutores recursivos, como se los conoce, no están bien protegidos. Son vulnerables. Imagínense los miles de ISPs que están ahí en todas las regiones, algunos están operador por empresas pequeñas que no tienen demasiados recursos. Entonces tienen la infraestructura para operar, pero quizá no tengan los recursos para protegerse.

Cuando esos servidores no están lo suficientemente protegidos, los delincuentes entonces pueden abordarlos de diferentes formas. Una de esas formas, yo soy un usuario de un ISP que tiene un resolutor recursivo comprometido, envío una consulta, busco datos vinculados con, no sé, PayPal.com. Entonces recibo la respuesta correcta, pero como el servidor ya está comprometido, los delincuentes le van a agregar otra parte más a la información, y ese *bit* de información que va a tener va a

decir, “Oh, y de paso la dirección de IP para BankOfAmerica.com es esta”.

Y automáticamente yo lo que hago es actualizar la memoria caché de todos mis dispositivos, que va a ser el archivo *host*. Cuando esto sucede, ¿qué va a pasar con mi dispositivo? La próxima vez que yo quiera ir a bankofamerica.com, ¿dónde me va a llevar el dispositivo? Esto pasa durante un periodo de tiempo. Pero me va a llevar a la dirección IP que los delincuentes querían que yo visitara. Esta es una mala situación. No es para nada buena.

¿Qué es lo que va a pasar entonces? Yo voy a visitar el servidor operado por los delincuentes. Voy a ver el contenido que ellos quieren que yo vea, que en este caso va a ser un sitio *phishing* que va a ser igual al *Bank of America*. Y obviamente, sin ningún problema, le voy a dar mi nombre de usuario y mi contraseña, que la verdad que no va a ser bueno para mis finanzas personales, obviamente.

Existe otras formas en las que los delincuentes pueden hacer cosas como estas. Porque pueden comprometer directamente el dispositivo y cambiar, modificar la configuración del DNS. Entonces, ¿cuándo lo hacen? Lo vamos a ver después en un ejemplo, en un *botnet* que sucedió hace cuatro años, me parece. Si mi dispositivo está configurado para enviar consultas de DNS

a, no sé, por ejemplo, 1.1.1.1, cambian esa dirección acá o en el *laptop*, y en lugar de esa dirección legitima ponen la de ellos, ponen la propia del servidor del DNS que ellos operan, que está configurado para dar direcciones de IP a su propia infraestructura. En otras palabras, van a tener a todos los usuarios con un dispositivo comprometido, todos esos usuarios van a visitar sus sitios web, que obviamente no es agradable. Y después vamos a hablar de esto.

En un caso como este, sobre todo cuando hablamos de envenenamiento del caché, tienen el dispositivo comprometido que envía la consulta a su servidor de DNS. Yo estoy buscando un sitio que no es importante para los delincuentes, lo que sea, uno nuevo. Pero digamos que este sitio no es importante para los delincuentes. Como hicieron en el ejemplo anterior que yo les di, le agregan otra parte de información a la respuesta, para que los servidores de ellos le envíen a mi dispositivo, y esa información puede ser similar a la dirección IP – oh, y además si quieren la dirección para su banco es esta. Entonces, dentro de un periodo definido, yo voy a hacer una consulta para ese nombre de dominio de mi banco porque quiero hacer banca en línea, y termino en el sitio web de los delincuentes. Y, nuevamente, esto afecta a mis finanzas personales.

DNSChanger es exactamente el tipo de situación que les estaba describiendo. Eso es exactamente lo que hizo. Cambió la

configuración del DNS que pretendía el usuario. Y fue muy ubicuo, en realidad abarcó mucho. Utilizo esta *botnet*, las mentes maestras de esta operación pudieron ganar muchísimo dinero. Para cuando las autoridades de aplicación de la ley pudieron intervenir, pudieron demostrar con evidencia contundente que habían podido obtener 25 millones de euros de forma ilegal. Eso no significa que no hayan ganado más. Significa que eso es lo que pudieron demostrar las autoridades como evidencia.

Con DNSChanger los delincuentes cambiaron la configuración de los dispositivos del usuario. Hicieron algo que parecía ser bastante inocuo porque reemplazaron las publicidades que ven los usuarios cuando ingresan a los sitios web. Entonces si yo entraba a mi sitio de noticias preferido por la mañana en la oficina con mi taza de café, en lugar de ver las publicidades legítimas ellos habían reemplazado esas con otras. Y esto generaba también ingreso para ellos de forma continua. Esto ocurrió durante muchísimo tiempo, de modo que fue una máquina de hacer dinero.

No causó daño, parece. Los usuarios no vieron ninguna conducta extraña en los dispositivos. Los usuarios podían seguir accediendo al contenido que querían acceder, podían interactuar con Internet y con los recursos que necesitaban.

Entonces aparentemente, a simple vista, no había nada que estuviera mal.

Pero sí, lo había. O sea que se produjo esa acción y hubo tantos dispositivos infectados, no recuerdo la cantidad exacta, pero eran cientos de miles de dispositivos que se vieron comprometidos por esta *botnet*, por este tipo de actividad maliciosa en muchos países. Podrían ser 20 países, pero no estoy del todo seguro acerca de la cantidad de países afectados.

Entonces se planteó una pregunta cuándo ellos, me refiero a las autoridades de aplicación de la ley, iban a tener que hacer algo con estos servidores DNS con los que estaban operando los delincuentes. Podían desactivarlos, en cuyo caso, ¿qué creen que hubiera pasado si hubieran apagado esos servidores? Todos los dispositivos de los usuarios estaban enviando consultas a esos servidores, ¿qué hubiera pasado si los desactivaban?

Los usuarios habrían pensado que habían perdido la conexión de Internet. Seguirían conectados a Internet, pero sus dispositivos no iban a traerles ninguna respuesta porque los servidores DNS iban a estar apagados, entonces no los podían apagar.

Entonces lo que hicieron fue utilizar la ingeniería para reemplazar esos servidores. El administrador de esos servidores durante un tiempo utilizó distintas técnicas y hubo campañas de

sensibilización que se hicieron en las distintas jurisdicciones para que los usuarios se dieran cuenta de que tenían que hacer una limpieza, un análisis de sus dispositivos.

Por supuesto, dado que los delincuentes han encontrado distintas maneras de abusar del protocolo de DNS y de utilizar para fines ilícitos las distintas operaciones del DNS, es interesante, por lo menos desde la perspectiva académica, ver que esto muestra creatividad para malos fines, pero son muy creativos. Como por ejemplo el canal de exfiltración encubierto. Creo que este es el siguiente ejemplo.

Aquí tenemos un canal de exfiltración encubierto que se produce cuando se envían datos de una red comprometida sin que el administrador de la red se dé cuenta de que le están robando sus datos. Esa es la parte encubierta. Y el DNS es considerado un canal de exfiltración realmente muy bueno como encubierto porque hay un puerto pequeño que se utiliza para DNS para las comunicaciones y no se bloquea. No puede ser bloqueado.

Entonces el tráfico en las redes se traslada de un puerto a otro a través de estos puertos. Los puertos que se utiliza el protocolo de DNS es el Puerto 53. Si bien hay formas en que los ingenieros pueden reasignar ese puerto internamente dentro de la red, puede generar algunas complicaciones. Entonces, por lo

general, nunca se vuelve a asignar, nunca se traslada a otro puerto. Eso significa que el tráfico por el Puerto 53 no puede bloquearse. Es muy complicado para reasignarlo. Y no se puede bloquear. Si se bloquea, no pueden tener la resolución de DNS, lo cual significa que las personas van a pensar que están bien.

Ahora, ¿cómo funciona cuando tenemos un canal de exfiltración encubierto? Bueno, de distintas maneras, por lo menos hay dos que se me ocurren en este momento. Una es, se compromete un dispositivo y ese dispositivo comienza a enviar consultas lentamente a un servidor de nombres de los delincuentes. Lo que pasa es que dentro de cada una de esas consultas del DNS los delincuentes reemplazan los bits más relevantes con aquellos que están exfiltrando. Entonces las consultas de DNS siguen siendo consultas del DNS. Si el equipo de ingeniería o el administrador de la red está analizando esas consultas en el trafico van a ver que son consultas del DNS. Pero van a tener que recolectar todas esas consultas DNS que están utilizándose para la exfiltración de esos datos específicos, las van a tener que reunir y se requiere mucho análisis básicamente. Se tienen que dar cuenta de que hay algunas piezas que están siendo reemplazadas y tratar de dilucidar qué es lo que está ocurriendo y cuáles son los datos que se han exfiltrado. Esa es una manera.

Otra manera en la que los delincuentes, que es un poco más fácil, utilizan el DNS para exfiltrar los datos es a través de registros. Uno tiene que administrar un archivo de zona.

En el archivo de zona con el nombre de dominio uno encuentra los recursos que están vinculados con ese nombre de dominio. Allí se incluye la información del sitio web, del servidor FTP, del servidor de correo electrónico. Si tienen una firma de DNSSEC la información va a ir ahí. Si tienen otras tecnologías, otras técnicas para proteger a los clientes, o la red, puede estar allí. Hay más siglas, lamentablemente. Tal vez escucharon hablar de SPF, DKIM y DMARC, que eso se utiliza para proteger la red.

Todo ese tipo de información termina en lo que llamamos registros de textos. Y podemos poner cualquier cosa en esos registros de texto. No hay limitación con respecto al tipo de texto que pueden tener esos registros de texto. Es simplemente texto. Entonces los delincuentes utilizan esos registros de texto para exfiltrar información también. Pueden enviar consultas con información sobre esos registros de texto a cualquier servidor que recaba esta información, la pueden agrupar, recrear los datos que fueron exfiltrados, etc.

Y el flujo rápido. Creo que esto se mencionó, pero creo que ya fue mencionado, el *fast flux.*

Tenemos las registraciones de nombres de dominio que son un blanco atractivo para los atacantes, por supuesto. Lamentablemente hay abusos que se han cometido en este espacio, en el espacio de los ccTLDs. Les encanta hacer abuso de los registradores, de los revendedores, tener acceso a gran cantidad de nombres de dominio. Es un problema muy complicado de resolver. Los precios más bajos de los nombres de dominio tienden a estar vinculados con personas que actúan mal. Esta es la naturaleza humana. Uno busca lo más barato y así ellos pueden vender muchos de estos nombres de datos. Los registratarios y los usuarios legítimos muchas veces van a buscar el precio más bajo y terminan con estos nombres de dominio que no son lícitos.

Este tipo de abusos de las registraciones es parte de cómo ha evolucionado la industria y ahora hay muchos de estos nombres, pero los atacantes los abusan y cuando menciono estoy pensando en los dominios DGA, que son aquellos que están en las manos de los atacantes para poder generar muchos de estos nombres de dominio.

DGA es Algoritmo para la Generación de Dominios. Entonces utilizan una infraestructura los delincuentes para poder mandar y controlar esa infraestructura.

Y, ¿qué pasa si esta estructura se cae? Tienen que tener un plan B, C, D, E, F, G, etc. Ahí entran los DGAs. Cuando el *botnet* se da cuenta de que uno de esos servidores asociados con el comando y el control está desactivado, no está funcionando, genera – esto es un ejemplo, porque tenemos todo tipo de variantes aquí de conducta de DGA. Esta es una explicación más simplificada de cómo se utiliza este algoritmo. Entonces se activa una nueva cadena de caracteres para ese TLD y empieza a funcionar.

Si pueden controlar esa situación en la *botnet* por una acción de litigio, de amenaza, allí se pierde la funcionalidad de control y comando por este algoritmo y puede seguir funcionando.

Vamos a mencionar un caso muy interesante. Espero que estemos llegando ya a esa diapositiva. ¿Por qué los atacantes y los delincuentes registran los nombres de dominio? Para todo lo que se les pueda ocurrir, para suplantación de identidad, para *ransomware*, para *malware*, para vender productos farmacéuticos de manera ilegal, productos falsificados; para todo lo que se les ocurra.

Y la última viñeta acá, que no sé por qué no aparece, corresponde a comando y control, que tiene que ver con la estabilidad y con la flexibilidad, que son las preocupaciones más grandes que tenemos por el tamaño de estos ataques.

A veces hay preguntas con respecto a los productos farmacéuticos ilegales, si esto tiene que ser considerado abuso del DNS o si está vinculado técnicamente con el abuso del DNS. Y esto se parece más a la situación de los sitios web falsificados. Y es cierto, pero a veces hay algunas cosas subyacentes por debajo de la superficie, no puedo entrar en todos los detalles ahora, pero tengan en cuenta que hay algunas coas que están por debajo de lo que ustedes ven a nivel superficial. Tal vez ustedes ven que simplemente se trata de algunos sitios web que se utilizan para enviar de manera ilegal medicamentos, lugares donde están prohibidos, pero muchas veces por debajo de esa superficie hay otro tipo de perjuicios y de situaciones que se cometen.

¿Tienen alguna pregunta? Acérquese al micrófono si tiene una pregunta, por favor.

CATHY PETERSEN: Pueden usar cualquier micrófono que esté en la mesa. Díganos su nombre y a dónde pertenece.

FARZANEH BADII: Soy Farzaneh Badii. Soy la Presidenta del Grupo de Partes Interesadas No Comercial. Pregunto a título personal. Cuando ustedes dicen que debajo de un nombre de dominio que vende

medicamentos en forma ilegal puede haber otras situaciones malas, ¿están hablando de algún abuso de índole técnica o estamos hablando del contenido?

CARLOS ÁLVAREZ: Estoy hablando de operaciones criminales que pueden usar estos nombres de dominio. Tiene que ver con el contenido del sitio web y más actividad criminal que sigue a partir de allí.

FARZANEH BADII: Entonces, ¿esto no tiene nada que ver con las operaciones técnicas del DNS?

CARLOS ÁLVAREZ: Tiene que ver con el uso del nombre de dominio.

Entonces, ¿por qué van a pagar los criminales por los nombres de dominio si en realidad los pueden robar o pueden controlarlos de alguna otra manera?

Hay distintas situaciones en las que los delincuentes pueden acercarse a estos nombres de dominio en lugar de simplemente secuestrar un dominio. ¿Cómo lo hacen? Pueden comprometer el uso de las credenciales de acceso de los registratarios a través del panel, que es la interfaz que permite a los registratarios administrar su nombre de dominio.

Imaginen una organización de delincuentes que quiere tomar el control de un nombre de dominio de mucho valor o quieren causar daño a los clientes de un banco especifico. Pueden tal vez enviar una campaña de suplantación de identidad, de *phishing*, pueden dirigirla a los empleados de ese banco, después de algún trabajo de ingeniería social como es habitual, pueden atraer a los empleados de ese banco a hacer clic en algo que no deberían hacer clic y allí pueden robarles sus credenciales de acceso.

Y todo lo que ocurre después de ese punto llega tanto como quieran los delincuentes. Pueden crear simplemente un dominio de tercer nivel debajo del dominio de segundo nivel. Si mi banco ha sufrido una situación de este tipo -- digamos el banco de “carlos punto lo que sea”, el delincuente puede crear una dirección similar en otro nivel y puede enviar un correo electrónico como parte de una campaña de *phishing*, atraer a las víctimas de manera más exitosa porque el nombre de dominio de segundo nivel es el nombre de dominio real de mi banco.

O pueden modificar los servidores de nombre completamente o cualquier información que esté asociada con el nombre de dominio. Pueden modificar. Y los registros pueden dar de baja todos los registros y poner su propio archivo para ese nombre.

Hay situaciones que se han dado donde los registradores que tal vez no tienen su infraestructura bien protegida se han visto comprometidos. No es que haya pasado muchas veces, pero ha pasado. Pero cuando pasa, no es una buena situación. Afortunadamente, en esos pocos casos que hemos visto, los delincuentes apuntaron a blancos de alto volumen muy específicos y los registradores pudieron responder rápidamente. Eso fue hace un tiempo. Se manejó de manera adecuada. Pero los delincuentes buscaban blancos específicos, querían hacerse con el control de determinados servidores.

Del lado de los usuarios, si los registratarios son atraídos a hacer clic en algo que no deben a través de un ataque de *phishing* que es exitoso o son atacados a través de su registración y la infraestructura de la registración, allí pueden tener éxito.

Lo que estaba mencionándoles. Este es otro aspecto del *phishing*. Los registratarios, ¿cuántos de ellos podrían tener credenciales de acceso al panel de control para administrar los nombres de dominio? ¿Cuántos registratarios van a tener las mismas credenciales de acceso en ese panel de control como en una cuenta que se había comprometido antes? Cualquiera de estas grandes situaciones se ven todos los meses, todas las semanas. ¿Cuántas? Eso se desconoce.

Los delincuentes tratan de conectarse en tantos servidores como puedan con el nombre de usuario y la contraseña que fueron robados a través de otras violaciones a la seguridad. Cuando ingresan, ya está. Se terminó todo. Y eso es un gran signo de pregunta. No hay forma de probar eso, de cuántos registratarios están utilizando sus antiguas contraseñas para el manejo de sus registraciones de nombres de dominio. Entonces hay que ser muy conscientes de lo que se hace.

Acá estaba lo de *Fast flux.* Esta es una técnica que utilizan los delincuentes para pasar de una dirección de IP a otra rápidamente, para que entonces los profesionales de la mitigación de riesgo y las autoridades de aplicación de la ley no los puedan encontrar.

Lo pueden definir dentro de sus archivos dentro de TTLs. TTL es el tiempo de vida útil. EL TTL es donde una dirección de IP que está asociada con un sitio web es válida. Después los resolutores recursivos salen y no van a poder obtener consultas nuevamente. Y cuando lo hagan, le van a dar una dirección IP diferentes. Entonces cuando vemos TTLs muy cortos, de 120 segundos, 180 segundos, 2 o 3 minutos, o 4 minutos, hay algo entonces que el registro tiene que mirar como diciendo, “Hmm”.

Acá la advertencia es que los CDNs largos que son las redes que entregan contenido, tengan su propia operación para dar

estabilidad y todo lo que tenga que ver motivos técnicos para usar TTLs. En ese caso las cosas son diferentes porque si uno es un investigador y sabe cuáles son los TTLs que utiliza esta red que puede ser muy grande. Ahora, si es un nuevo dominio y tiene un TTL corto vinculado con una nueva infraestructura que no se vio o asociada anteriormente y que ahora está asociada con spam, entonces esa es una señal de alerta. Y, en general, entonces los investigadores de la red suelen bloquear todo lo que tiene que ver con la investigación de esta infraestructura para protección.

Qué es lo que pasa entonces cuando uno es una autoridad y está investigando una infraestructura delictiva, que están utilizando *fast flux*. Ustedes pueden ver que el contenido está en este servidor en este país, minutos después el contenido ya no está acá, sino que está en otro servidor, en este otro país. Dos minutos país pasa a otro país, a otro servidor; dos minutos después el contenido pasa a otro servidor. Cuarto o quinto país, etc. ¿Cómo entonces las autoridades lo hacen con esto?

Es muy difícil. Muy difícil. El doble *fast flux*, como está acá abajo, es una técnica que se vio en una nube muy grande, como lo diría. En un servicio de nube de delincuente que se llama Avalanche. Dentro de Avalanche, los delincuentes hicieron un doble *fast flux*. Es decir, cambiaron los nombres de los servidores con mucha velocidad.

Entonces si yo quería hacer una consulta con carlos ahora, ahora lo haría en este ns1.carlos.loquesea. en dos minutos iba a hacer otra consulta y podía ser en ns1.cathy.next, pero en los dos minutos siguientes era ns3.cameron.yoohoo. Cada dos minutos entonces cambiaban los servidores de nombres. Y los servidores de nombres estaban por encima de eso, cambiando cada dos o tres minutos sus direcciones de IP. Esos TTLs cortos que habían definido los delincuentes. Es el doble de malo, el doble de complicado, pero los buenos investigadores pudieron encontrarlo y ahora gracias a Dios los delincuentes ya están tras las rejas, también su cabecilla.

Yo hablé también del DNS como un canal de exfiltración encubierto. Este es un tipo de moderno no sólo de exfiltración sino básicamente también para el control real del módulo del malware que se ve afectado en los dispositivos. Entonces a través del DNS los delincuentes les dan instrucciones a los dispositivos. Los delincuentes pueden inyectar este software malicioso dentro de los dispositivos a través del DNS.

Es un dolor de cabeza porque, como dije, el Puerto 53, que se utiliza para las comunicaciones de DNS, no puede bloquearse. Entonces es el administrador el que tiene que tener buenas técnicas para detectar este tipo de cosas.

Hay algunas técnicas que pueden utilizarse. no puedo hablar de esto ahora porque sería otra sesión de tres horas. Pero es cada administrador de red el que tiene que decir qué técnicas aplica.

Esto ya lo vimos. Acá son dos ejemplos de software malicioso que están haciendo esto entre otras cosas. Estos son Morto y Feederbot. Acá pueden ver cómo hay una instrucción para las respuestas TXT del DNS. Acá el delincuente configuró este servidor del DNS para que dé una respuesta a la consulta recibida porque la consulta fue por un registro TXT y en realidad ahí se llevan instrucciones para comprometer al dispositivo que realizó la consulta. Y esas instrucciones pueden ser cualquier cosa. Pueden ser, "Ataque estos blancos o este tráfico de esta forma". Cualquier cosa.

Vamos a ver entonces cómo evoluciona todo este panorama en las amenazas al DNS. Hablábamos del DDoS como servicio. No sé tampoco si se acuerdan de Mirai. ¿Alguien se acuerda? Bueno, fue una muy mala situación.

Mirai en realidad – a ver, cómo lo explico. Había una asociación entre los proveedores de lo que se llaman servicios *booter* o *stresser* y hubo un ataque con estas *botnets*.

¿Qué es un *booter* o un *stresser*? Es un sitio web donde alguien lo establece en algún lugar y dice que venden la capacidad de hacer pruebas para ver si sus servidores son flexibles y estables.

Entonces se le paga un cierto dinero y dicen que venden y dicen que van a hacer, “vamos a mandar este tráfico durante este tiempo para verificar la infraestructura, para ver si es flexible, para ver si puede soportar un ataque”.

El tema es que estos servicios de *booter* o *stresser* se lo venden a cualquiera, operan en la infraestructura que van a probar o no. En otras palabras, en realidad son servicios que se alquilan y no es difícil encontrarlos. Porque aparecen en línea, aparecen fácilmente entre los proveedores que se ofrecen y el tema es que algunos aceptan tarjeta de crédito para el pago, y lo único que tienen que hacer es pagar y darles la información, el blanco que quieren probar, porque obviamente quieren ver que la red sea flexible. Esto no está bien.

Lo hacen a través de diferentes medios, uno es lo que son obviamente las *botnets* operativas. Ya estuvimos hablando de *fast flux* y doble *fast flux*. Mencioné Avalanche. Hablaremos de ello después, pero fue un caso muy particular y van a ver por qué.

La Internet de las Cosas. No quería mencionar la palabra que está entre “Internet de” y “Cosas”, pero la “palabra v” que está ahí no es nada nuevo y es vulnerable.

Las cosas pueden salir mal. Piensen en el ataque, me parece que fue contra Brian Krebs en octubre o septiembre del 2016, frente

a OVH. OVH es un registrador realmente que también da muchos servicios de hosting en Francia. Ellos pudieron detectar que el ataque venía de algo que tenía cerca de 146.000 cámaras de vídeo.

Entonces la *botnet* podía enviar 1.5 terabytes de datos. Era algo que no se había visto, porque esa cantidad de datos, la verdad, yo no me lo pude imaginar en mi cabeza. Pero tenía que medir 1.1 terabytes en tráfico directo que les llegaba. Y eran de cámaras de vídeo. No era nuevo, pero es algo que vale la pena mencionar. El DNS fue uno de los vectores que se utilizó en ese ataque, no el único, pero sí uno de los vectores utilizados.

Y después tenemos WannaCry, que por ahora lo voy a dejar de lado.

Avalanche fue un servicio de delincuencia en la nube. Imagínense que van a un sitio web, generan una cuenta, se registran, ingresan, eligen entonces el tipo de campaña que quieren hacer. Lo que hizo esta gente fue hacer todo por ustedes. Ustedes nada más que tenían que pagarles algo, y ellos hacían el resto. Les daban también el software malicioso, ellos infectaban a los clientes por ustedes. También hacían comando y control en nombre de ustedes.

Hacían un rastreo, les daban el hosting para los sitios de distribución de software malicioso. Todo lo operaban por

ustedes. Fue el siguiente nivel de sofisticación, obviamente porque brindaban servicios criminales.

Avalanche obviamente tenía mucha registración DGA en dominios generados por un algoritmo. Cuando se dieron cuenta las autoridades de aplicación de la ley se aproximaron a la ICANN. Esto se llama un pedido. Después de eso se sacaron 832.000 nombres de dominio de las manos de los delincuentes.

Gracias a toda la cooperación que existió en ese momento de las autoridades de aplicación de la ley y gente del sector privado, los delincuentes perdieron el control de su infraestructura. Desapareció. Está ahí, pero no los pueden tocar. No los pueden controlar. Y realmente se siente bien cuando estas cosas suceden. Uno se siente contento.

Estas son algunas de las cadenas de caracteres que fueron creadas por Avalanche, por la *botnet*, para el comando y control. Si bien tenemos esos 830.000 que estaban creados debajo de todos estos TLDs, tanto ccTLDs como gTLDs. Porque como dije, los delincuentes abusan de quien sea. No les importa, obviamente.

Y hay algo más. Algunos delincuentes en algunos lugares del mundo van a generar un software malicioso para que no ataquen a sus direcciones de IP dentro de su propia jurisdicción porque no quieren que los persigan las autoridades y entonces

eso sería malo. Entonces lo que hacen es saltear completamente lo que es su espacio de direcciones IP.

El tema es que no pueden dejar su país, lo que en sí mismo es algo malo. Entonces son prisioneros de sí mismos dentro de sus propias fronteras. Es bueno que se queden ahí, pero en realidad hace mucho daño al resto del mundo.

Estos son los resultados de Avalanche y de lo que pasó. Gracias al contenido que dio Europol y el FBI podemos hablar de este caso en la presentación. Acá presenta nada más que las cifras de los resultados. Cinco arrestos en cuatro países. 37 búsquedas en siete países, 39 servidores tomados en 13 países, 221 servidores salieron de línea, 64 TLDs/832.000 dominios en 26 países. Y, obviamente, también recuperación a las víctimas y aumentar la concienciación y prevención. Esta realmente fue una operación a gran escala. Fue algo bueno, realmente un gran golpe.

WannaCry fue algo raro desde la perspectiva del DNS. Fue interesante, a diferencia de lo que se ve habitualmente en lo que tiene que ver con tipos de software malicioso que utiliza los nombres de dominio para comando y control dentro de cualquier TLD, gTLDs o ccTLDs -- comando y control. En el caso de WannaCry se dio a través de distintos nombres de dominio. No sé si ustedes saben que .onion se definió como uno especial, o sea que nunca podía estar en la raíz. La ICANN nunca iba a

tener nada que ver con este .onion. No había forma entonces de sacar la infraestructura de comando y control asociado con WannaCry.

Sin embargo, este investigador joven, Marcus Hutchins, un chico británico, estaba analizando el código. Pudo obtener un ejemplo de WannaCry. Encontró una cadena de caracteres que creo que estaba dentro del código, obviamente estaba dentro del software malicioso. Entonces lo buscó. No estaba registrado. Lo registró y paró la diseminación de este software malicioso. DE casualidad. No tenía idea de lo que iba a pasar. Pero con ese nombre de dominio paró la diseminación de este software malicioso.

Y la razón está acá. Si mi *ransomware* no puede conectarse con comando y control, entonces puedo evitar el análisis. Afortunadamente, estaba ahí. Y entonces se empezó a parar la diseminación de WannaCry.

Los delincuentes por detrás de WannaCry trataron de registrar una segunda cadena de caracteres, pero fue descubierto rápidamente. Y entonces se pudo detener la diseminación y se tuvieron que ir.

El abuso del DNS es un tema controvertido dentro de la ICANN porque hay diferentes puntos de vista. Algunos dicen que tiene que ver con la seguridad, con los organismos encargados de

aplicar la ley, también tiene que ver con la exactitud del WHOIS, de cómo se opera, cómo va a ser la apariencia del WHOIS después del 25 de mayo, cuando empiece a tomar vigencia el GDPR.

También hay preocupaciones que tienen que ver con el tiempo para las repuesta, cuándo se reacciona, cuándo hay un informe de abuso que se presenta. Hay distintos tipos de preocupaciones al respecto.

Por el otro lado, que es el lado en el que nosotros como organización también tenemos que escuchar, está la preocupación de que la ICANN no debe salir de su mandato, no debe salir de su alcance, es decir, que si es el contenido la ICANN entonces no tiene nada que ver con eso. Eso se traduce en que los contratos de la ICANN no incluyen disposiciones que hablan de sacar un contenido que tenga que ver con cuestiones sensibles. Eso es algo que tiene que ver con la comunidad y no con la organización. Y son ustedes la comunidad los que tienen que hablar de estos temas. Entonces nosotros no podemos participar en esas deliberaciones, si bien podemos facilitarlas.

Es importante el trabajo que hace el Grupo de Trabajo de Seguridad Pública, que es donde se alojan todas las autoridades de aplicación de la ley, donde está dentro de la estructura de la ICANN todo lo que tiene que ver con los comités que se ocupan

de estas cuestiones. Antes del PSWG, antes de que existiera, la comunidad de las autoridades de aplicación de la ley no había encontrado un lugar. Creo que hasta la reunión de Beijing, cuando Laureen Kapin de Estados Unidos y Fadi Chehade, en ese momento Director Ejecutivo, decidieron considerar tener un lugar formal para la participación de los organismos de aplicación de la ley dentro de la ICANN. Y allí le dijeron a la comunidad: "Tráigame una propuesta". Y eso hicieron. Y esa propuesta es lo que hoy es conocido como PSWG, que es un grupo de trabajo o un sub-grupo dentro del Comité Asesor Gubernamental. Allí residen.

El propósito del PSWG es dar asesoramiento al GAC y a la comunidad de la ICANN en su conjunto. Algunos de los temas en los que se concentran son el abuso del DNS, las formas en que los nombres de dominio se utilizan para fines maliciosos, para causar daño a los usuarios; el GDPR, que nos guste o no va a tener una implicación sobre la información de WHOIS que está disponible para la investigación y las búsquedas. También la traducción de direcciones de red de CGN NAT. Esta es una técnica que algunas ISPs utilizan cuando prefieren no migrar a IPV6, por ejemplo.

En lugar de tener que hacer esa migración a IPv6, generan redes de área local muy grandes y ponen allí las direcciones de IP. Las direcciones de IP que solamente tenían que estar en la Internet

publica, que nosotros las veríamos si estuviéramos analizando el tráfico, y direcciones que solamente tienen que existir en redes privadas que nunca deberían verse en la Internet pública. Lo que hacen, y esta es la situación, por ejemplo, en su compañía o en sus casas, sus dispositivos tienen asignados esas direcciones IP privadas.

Los ISPs les asignan esas direcciones privadas a sus clientes, aunque sean 500, 1000 o 10000, y generan a nivel del barrio redes privadas, son redes de área local con una única dirección IP pública. Eso genera una complicación para los organismos de aplicación de la ley, porque cuando ellos golpean a las puertas de una casa par entregar algún documento o una citación a un ISP para pedirle la información sobre el usuario que envió tráfico desde esta dirección de IP en esta fecha y en esta hora, el ISP le va a decir: “Bueno, no lo sé, son 10000 usuarios los que utilizan esa dirección pública de IP”.

Y en muchos países no hay obligación o tal evz exista la obligación, pero no se aplica con respecto al mantenimiento y el almacenamiento de distintos registros de información de inicio de sesión y cierre de sesión. Ya ahí no se guarda la información y el ISP no tiene registro de ese paso por ese lugar. Esto se discutió mucho en el pasado. El *fast flux*, que es una técnica que utilizan los delincuentes.

Estos son dos ejemplos muy sencillos. De ninguna manera es algo exhaustivo o restrictivo. Son disposiciones contractuales dentro del contexto de la ICANN. La red más amplia de contratos que tiene la ICANN. Puede haber muchos más. Podemos tener toda una conversación de varias horas para hablar del anti abuso desde el punto de vista contractual dentro de la ICANN.

Puedo mencionar que los registros tienen la obligación de monitorear sus zonas para ver si hay amenazas a la seguridad. Es decir, tienen la obligación de analizar los dominios que existen dentro de ellos.

Si yo fuera el TLD de .carlos, tendría que buscar todos los nombres de dominio allí y ver cuáles son sus suplantaciones de identidad, spam, software malicioso, comando y control, y los tendría que informar esas métricas y estadísticas a la ICANN. Esa es la obligación del lado de los registros.

Si no me equivoco, creo que los registros también tienen que proporcionar la información de abuso del punto de contacto.

Del lado de los registradores, hay un poco más de especificidad. Y estas disposiciones mas especificas están allí en ese acuerdo que se llama el RAA, que es el Acuerdo de Acreditación de Registradores. RAA es el nombre que usamos informalmente.

Estas disposiciones más específicas han sido incluidas como resultado de las recomendaciones de los organismos de aplicación de la ley que fueron presentados por lo que ahora es el PSWG, pero en ese momento simplemente era la comunidad de las autoridades de aplicación de la ley, eso fue en la reunión del 2012 en Costa Rica. Creo que allí se presentaron esas 12 recomendaciones.

Y eso hizo que la junta directiva iniciara las negociaciones con los registradores. Esas negociaciones llevaron meses y resultaron en el RAA del 2013 con algunas cláusulas un poco más específicas sobre medidas anti abuso.

Algunas tienen que ver con cuestiones que todavía requieren más claridad, a la comunidad le gustaría ver que algunas de las disposiciones son todavía más estrictas, pero en ese momento los órganos de aplicación de la ley estaban de acuerdo con este texto que fue acordado por la Organización de ICANN y por el Grupo de Partes Interesadas de Registradores.

Entonces, rápidamente, hablando de esto, aquí se incluye que los registradores tienen que tomar acciones razonables y rápidas para investigar y responder apropiadamente a cualquier informe de abuso. Tienen que publicar también los procedimientos para la recepción y el manejo y el seguimiento de esos informes. Y también tienen otra obligación que es la de

dar el punto de contacto para abuso. Esa información tiene que estar publicada en su sitio web, si no me equivoco, y/o en los datos de WHOIS. Creo que en los datos de WHOIS también tienen que publicarlo en sus sitios web también. No estoy seguro. Creo que tiene que estar allí, pero no estoy del todo seguro.

Hay una disposición también interesante allí, que es específica a los organismos de aplicación de la ley. Cuando un organismo de aplicación de la ley desde la misma jurisdicción de un registrador envía un informe de abuso a ese registrador, pero recuerden que esto tiene que estar dentro de la misma jurisdicción, el registrador tiene que dar una respuesta humana dentro de las 24 horas. Esa respuesta tiene que ser dada por un humano, no en forma automática. Esa respuesta no tiene que ser, "Suspendemos el dominio". Puede decir, "Hacemos acuse de recibo".

Y la persona que da esa respuesta, según este acuerdo, tiene que ser alguien que básicamente pueda decidir qué es lo que va a ocurrir con ese informe de abuso; si se debe suspender o no ese nombre de dominio.

Hay algunas jurisdicciones en las cuales esta cláusula es muy útil, hay muchos registradores que operan en esa misma jurisdicción, pero hay otras jurisdicciones en las que hay muy

pocos registradores o no hay ninguno. Entonces la eficacia o los efectos de la aplicación de esta cláusula varía según la jurisdicción de la que se trate, por supuesto.

Luego los prestadores de servicios de privacidad y representación o proxy, que los usan los registratarios para tener a alguien en su lugar, alguien más como información en el WHOIS en lugar de ellos mismos. Si yo no quiero tener mi nombre o mi dirección allí publicada, utilizo un proveedor de servicios de privacidad y representación que son controlados por los registradores, también tienen que dar su propia información del punto de contacto en caso de abuso.

Creo que eso es todo. Estos son los temas que yo quería cubrir con ustedes. Es mucho. El abuso del DNS parece ser un tema sencillo en el sentido de que cuando uno ve un nombre de dominio que se utiliza para el comando y el control de una *botnet*, claramente es eso. Es abuso. Pero cuando lo vemos, uno puede hacer todo el análisis técnico y no hay manera de ir en contra de la evidencia técnica que se presenta allí porque está allí. Pero luego hay otras situaciones, otros casos en los que se torna todo mucho más complicado.

Por lo tanto, es un tema que está siempre sobre la mesa para ser discutido en forma continua, para que la comunidad siga explayándose y expandiendo el conocimiento sobre este tema.

Al principio no lo dije, pero nuestra función – yo soy Director de Seguridad, Estabilidad y Flexibilidad con el Equipo encargado de estos aspectos. Estoy en la Oficina del CTO. Trabajamos con las autoridades de aplicación de la ley.

Hacemos muchas cosas. Tratamos de vincularlos más con la comunidad de la ICANN. Queremos que ellos entiendan todas las discusiones que se llevan a cabo aquí. Hace unas pocas semanas, un representante de la industria de nombres de dominio asistió a una conferencia de seguridad por invitación nuestra. Este era Jonathan Frakes, Director Ejecutivo de la Asociación de Nombres de Dominios. Hubo interacciones muy positivas en esa reunión.

Y esa es una de las cosas que hacemos. Nos relacionamos. Tratamos de traer a aquellas personas que se han visto tradicionalmente como lados contrarios, lados opuestos, para que lleguen a un terreno común, para que entiendan que se puede construir algo sobre la base de ese terreno común.

También trabajamos con los organismos de aplicación de la ley. Uno de nuestras funciones en la ICANN es mantener la estabilidad, la seguridad y la flexibilidad del sistema de nombres de dominio, entonces eso significa que las autoridades de aplicación de la ley tienen que entender qué significa cuando ellos están haciendo una investigación de un caso de *botnet* o de

software malicioso. Nosotros los ayudamos a entenderlo desde la perspectiva técnica para que ellos también se mantengan alejados del sistema sin interferir en él, aunque usamos a veces otros términos para definirlo.

Bueno, eso es todo. Si tienen alguna pregunta, por favor, siéntanse libres de hacerla.

CATHY PETERSEN: Por favor, digan su nombre y de dónde vienen si tienen alguna pregunta. Gracias.

[MARSY SURMO]: Hola. Soy [Marsy Sumo] de India. Tengo una pregunta y un comentario. La ICANN ha preparado algunas normas de seguridad basales para las operaciones de Internet. ¿Se podrían aplicar? Igualmente, aunque estén estas normas sigue habiendo ataques y este tipo de situaciones y siempre se puede hacer un análisis una vez que se ha producido el hecho. ¿Qué se puede hacer para poder prevenir el llegar a afectar la operación del DNS?

CARLOS ÁLVAREZ: Le sugiero que se fije en los documentos que se han publicado en DNS-OARC, que es la comunidad de los operadores de DNS,

donde allí pueden tener algunos componentes de seguridad para el DNS. Busquen M3AAWG. Esa es la abreviatura.

Hace un año y medio actualizaron lo que se conoce con el nombre de – y ahora no lo recuerdo. Si ustedes buscan con esta sigla y después DNS amenazas, lo van a encontrar. Y ahí van a encontrar muy buena información.

Esas son las comunidades o los grupos que yo creo que han trabajado en documentos o normas como las que usted menciona.

[MARSY SUMO]: Yo busco algún tipo de orientación, algún tipo de pauta general para asegurarnos de que se apliquen estas normas mínimas.

CARLOS ÁLVAREZ: Cualquiera puede operar un servidor de DNS en el mundo. No hay manera de hacerlas aplicar estas normas. Es imposible prevenir. No hay regla. No hay nada vinculante. Ellos pueden hacerlo como quieran. Lo hacen de forma voluntaria, lo cual no facilita las cosas, por supuesto.

Ahora, con respecto al comentario que usted hizo, si hablamos del componente voluntario, hay normas y formas de hacer las cosas que han sido definidas por la comunidad técnica desde

1997. Por ejemplo, el filtrado de las direcciones IPv4, por ejemplo, si se fijan en BCP 84 y en otras prácticas van a ver que están desde hace muchos años allí. Hay prácticas que no han sido implementadas tan ampliamente como uno esperaría, a pesar de estar en vigencia desde hace mucho tiempo porque son de adopción voluntaria.

¿Alguna pregunta más?

Adelante. Su nombre, por favor.

[HARU AL HASSAN]: Soy [Haru Al Hassan] de Nigeria. En los países en desarrollo tenemos un desafío: ¿cómo entrenamos a los organismos de aplicación de la ley para estar a la altura de estos delincuentes? Porque usted ha demostrado muchas maneras en las que se puede envenenar y atacar el DNS, de distintas maneras. Entonces, ¿cómo entrenamos a los funcionarios a cargo de la aplicación de la ley para poder estar a la altura de estos delincuentes?

CARLOS ÁLVAREZ: Creo que una ruta adecuada para hacerlo sería poniéndose en contacto con el personal de relacionamiento de la ICANN en África. No sé si usted ya los conoció aquí. Y expresarles su

preocupación con la persona que está a cargo de esas relaciones.

Esa persona con nuestro equipo de SSR va a coordinar y va a hacer que los organismos de aplicación de la ley participen en una capacitación que nosotros damos sobre abuso del DNS. Le sugiero que busquen a esta persona, Pierre, que realmente la preocupación que usted tiene es muy válida.

BRENT CAREY: Soy Brent Carey de .nz. La semana pasada yo vine de Ottawa y vi que había una cadena de caracteres de un nombre de dominio y había un abuso de registración y de infraestructura y de contenido. Y todo esto estaba surgiendo cada vez más. Entonces, ¿qué se puede hacer al respecto?

CARLOS ÁLVAREZ: Yo no sé, no tengo eso. Pero sé que [Bertrand] organizó ese foro en Ottawa. Algunos de mis colegas de la ICANN estuvieron allí.

BRENT CAREY: Porque hubo una ausencia de los organismos de aplicación de la ley allí.

CARLOS ÁLVAREZ: Está bien. Tomo nota de eso. Tal vez podemos hablar con el PSWG sobre esa situación en particular. Gracias.

Una pregunta más.

ORADOR NO IDENTIFICADO: Nosotros no tenemos un mecanismo sólido para cumplir con el GDPR de WHOIS. Y por otro lugar no tenemos control sobre estos temas de seguridad. Entonces va a ser muy difícil en el futuro, o al menos eso parece.

CARLOS ÁLVAREZ: ¿Qué es lo que va a ser difícil?

ORADOR NO IDENTIFICADO: Nosotros dijimos que no teníamos un auténtico WHOIS. Y entonces ahora vamos a ver el GDPR.

CARLOS ÁLVAREZ: Sí.

ORADOR NO IDENTIFICADO: No hay control sobre eso. No sabemos a dónde estamos yendo.

CARLOS ÁLVAREZ: Mi sugerencia es que participe entonces en todas esas deliberaciones, que dé sus comentarios. También lo que tiene que ver con las llamadas, porque es el Director Ejecutivo el que ha pedido comentarios al respecto. Entonces yo le digo que tiene que participar porque esa es la forma en la que pueden escuchar sus inquietudes. Y de hecho las escuchan, no es algo retórico lo que estoy diciendo, sino que sí se los escucha. Ustedes tienen inquietudes al respecto y son válidas.

Estas son algunas sesiones. No son las únicas que son importantes o que tengan relación con el abuso del DNS. Pero lo señalo acá en las pantallas. Si ven, ayer a las 11:30, si pueden volver en el tiempo, podrían haber visto lo que es el informe del PSWG. Después, mañana martes tenemos otra reunión del PSWG con el GAC.

Les pido que [Inaudible] el tema del GDPR. Es algo que nos encuentra en este cruce de caminos, entre las distintas cosas. Ambas reuniones van a ser muy importantes.

También hay que ver qué es lo que está haciendo la industria de nombres de dominio con su propia iniciativa, para ver qué es lo que están haciendo. Son cosas interesantes también.

Y después, DAAR. Esta es una herramienta que se está desarrollando y que da información sobre lo que son las malas registraciones o cómo esto se puede sumar a una parte en lugar

de otra. Y esto también es muy interesante realmente, porque acá van a poder ver mucho. Me interesaría que vayan a esa sesión, que participen y que se diviertan.

Bueno, muchas gracias a todos por haber estado acá.

CATHY PETERSEN: Para recordar: las presentaciones ya están en el cronograma público. Después también se van a subir las transcripciones y la grabación de esta sesión. Todo va a estar en el cronograma público en pocos días, así que cualquier cosa pueden remitirse a ello y ver todo nuevamente.

Muchísimas gracias. Ahora vamos a tener la siguiente sesión de Cómo Funciona a las 15:30 y no 15:15 como dice acá. Es Cómo Funciona la Red en Internet. Es un poco más tarde de lo previsto. Y en la sesión sobre el trabajo en Red de Internet se va a hablar sobre IPv4 e IPv6, sobre ambos protocolos.

Así que les pido que salgan, tomen un café y vuelvan acá a las 15:30.

Gracias.

[FIN DE LA TRANSCRIPCIÓN]