JOHANNESBURGO – Sesión de trabajo 5 del ALAC y los líderes regionales
Miércoles, 28 de junio de 2017 – 13:30 a 15:00 JNB
ICANN59 | Johannesburgo, Sudáfrica

ALAN GREENBERG: Gracias. Bienvenidos a la sesión número cinco. Tenemos varios presentadores y muy pocos minutos para cada uno. Comenzamos ya mismo. El primer orador es Greg Aaron. Perdón, estoy sin aliento. Vamos a hablar del uso indebido de los nombres de dominio. Greg es una de las personas que se ocupan de controlar las cosas feas que pasan por la Internet y, con suerte, nos protege. Va a ser una charla interesante. No voy a desperdiciar más tiempo en presentaciones.

GREG AARON: Gracias, Alan. Yo soy experto en ciberseguridad. Una de mis especialidades es observar cómo los delincuentes cibernéticos usan los nombres de dominio. Trabajo para una empresa de ciberseguridad que se llama iThreat. También soy miembro del SSAC. Soy fellow de investigación sénior en el grupo de trabajo sobre lucha contra el phishing.

Una manera de definir el uso indebido de los dominios es aquella actividad que requiere o usa un nombre de dominio para perpetrar actividades perjudiciales. Dentro de esta definición

hay bastante espacio de interpretación. Quisiera concentrarme en un fenómeno muy conocido, el conjunto central de ciberdelitos. Cada uno de estos usa los nombres de distintas maneras pero los dominios son fundamentales para poder llevar a cabo estas actividades.

En el centro tengo el spam. ¿Por qué lo puse en el centro? Porque es el que habilita los otros problemas. El spam lo definimos de manera tradicional. Es el correo electrónico a granel no solicitado. En algunas jurisdicciones quizá esto no sea estrictamente ilícito pero aquí yo me refiero a esa actividad que es ilegal en la mayoría de los lugares o que utiliza medios ilegales. El 85% de los mails enviados en el mundo son considerados spam. La mayoría es enviada por botnets que son redes de máquinas comprometidas que han sido hackeadas e infectadas con malware. Enviar spam por este método ya de por sí es algo muy mal. Es una actividad delictiva, construir un botnet o utilizarlo.

El spam también se usa para publicitar todo tipo de cosas. Algunas bastante inocuas. ¿Qué pasa? Aquí hablamos de dominios que son publicitados en el cuerpo del mail. Ese es el lugar al que el spammer quiere que uno que vaya, que entre. Por ejemplo, hay un vínculo en el mail. Esto consume toneladas de nombres de dominio por año. Estamos tratando de hacer un seguimiento del impacto pero aparentemente consume entre 8 y

10 millones de nombres de dominio únicos por año. De los 300 millones de nombres de dominio que existen en los registros, hay un porcentaje importante involucrado en esta actividad.

El spam, por ejemplo, se utiliza para publicitar phishing. Phishing es cuando un delincuente configura un sitio web que imita un sitio confiable, como PayPal o un banco. Quieren que la gente inserte los números de tarjeta de crédito, los nombres y otra información sensible que se almacena para cometer fraude contra las personas, para hacer extracciones de las cuentas bancarias y ese tipo de cosas. Así es como se publicita el phishing. Muchas de estas cosas no la ven en sus buzones de entrada porque hay muchísimas personas que intentan trabajar contra esto, y no siempre lo vemos en los buzones.

El spam publicita lo que llamamos los engaños de 419, como el engaño de Nigeria. Es también una manera de diseminar malware. Cuando alguien cliquea en algo y nos lleva a un sitio donde descargamos algo de manera consciente o inconsciente que afecta a la computadora. Ese malware se conecta con un botnet y nuestra máquina se usa para actividades que quizá desconozcamos. Los botnets, entre otras cosas, envían spam y se usan también para enviar ataques de DDoS, que son ataques de denegación de servicio, donde se envía muchísimo tráfico a un destino para perturbarlo y hacerlo caer. Las actividades de

DDoS se están incrementando. El ancho de banda que consumen también se está incrementando.

Habrán escuchando hablar de dispositivos de Internet como cámaras de seguridad y artefactos, equipos que se usan para actividades de ese tipo porque están infectadas con malware. Este es el conjunto central de actividades a las que suelo referirme porque están diseminadas en forma generalizada. Son conceptos bien entendidos y son básicamente actividades delictivas. Hay un consenso bastante generalizado al respecto en casi todo el mundo. La siguiente.

Este es un ejemplo del tipo de seguimiento que hemos hecho en el comité de seguridad. Este es el grupo de trabajo de lucha contra el phishing o la suplantación de identidad. Aquí muestra una relación entre los ataques de phishing y la registración de nombres de dominio. Estas son las estadísticas del número de ataques. En otras palabras, estas páginas o sitios particulares que se usan para perpetrar phishing han crecido cuatro veces. Se ha cuadruplicado desde que comenzamos a rastrearlo en el 2008. El número de nombres de dominio que se registran como phishers también está aumentando.

En 2016 fue la primera vez que vimos nombres de dominio registrados en cantidades tan importantes. Los phishers pueden violentar un sitio web. Proveedores de alojamiento también,

porque ellos también son víctimas. Ponen sitios de phishing en el sitio web de otro. Así es como la mayoría de las veces esto ocurre, a través de colapsar un sitio web de un tercero. En 2016 los phishers salieron a comprar nombres de dominio y gran parte de esta actividad está localizada en algunos lugares de la industria de los nombres de dominio. Ciertos registradores venden más que otros y algunas actividades de phishing ocurren en algunos TLD. Va cambiando pero en general ha sido así. Gran parte de la actividad se concentra en unos pocos lugares. La mitigación es una cuestión con algunos proveedores que son vulnerables de un modo u otro. La siguiente.

Ahora quiero referirme a algunas de las realidades que no solo los profesionales de la seguridad o quienes deben dar una respuesta conocen sino también cómo el mismo ecosistema está organizado. El resultado final es que estas actividades están diseminadas en forma generalizada. Los delincuentes que las perpetran son profesionales. Sin duda hay algunos aficionados pero gran parte de los que hacen esto ganan millones de dólares al año. Estos montos es dinero robado de personas y compañías que va aumentando a lo largo de los años. Las cuentas bancarias, grandes y pequeñas, son el blanco. No estamos hablando de unos pocos cientos de dólares por tarjetas de crédito. Estamos hablando de decenas de miles de dólares. Esa es la norma.

El uso indebido suele concentrarse en algunos lugares, algunos registros, algunos registradores y algunos proveedores de alojamiento. ¿Por qué es así? A veces no prestan atención. Quizá no tienen una persona que se ocupe de ver estos problemas. Es un problema de prevención. Es decir, conocer a los clientes y dejar a la gente que no queremos que esté, afuera. Una vez que saben que es un problema y que es reportado, también es una cuestión de ver qué se hace al respecto. Está el tema de ser proactiva como compañía, que estas actividades estén controladas o que se responda a estas situaciones cuando la gente las informa. Puede ser también que no se responda.

La falta de atención es un tema. En la industria de los nombres de dominio, los bajos precios es otro problema. Uno de los nuevos problemas es que los nuevos TLD, algunos nombres de dominio han sido muy baratos. Hay mucha competencia en la industria y millones de dominios fueron vendidos, específicamente los TLD, para hacer spamming. Ese es un tema porque los delincuentes no quieren pagar mucho, al igual que cualquiera. Cada tanto, en algunas de estas industrias hay cómplices o incluso actores que son delincuentes. En el espacio de los registradores ha habido muchas empresas registradoras que son propiedad de delincuentes que tienen como objeto perpetrar actividades delictivas.

Este [inaudible] es uno de estos registradores. ABSystems en Estonia fue condenado. Usaban el registro para hacer spam de un dominio que se vendía a empresas farmacéuticas. El responsable, después de ser arrestado por la DEA, admitió que había cancelado contratos con un par de personas. Son personas que conocen el sistema de nombres de dominio, que están en ello, y no juegan con las reglas de la sociedad normal.

La mitigación principalmente la hacen los privados, no los organismos de aplicación de la ley. La aplicación de la ley es muy importante pero las agencias no siempre tienen los medios para ocuparse de esto. Por supuesto, tienen que ocuparse de los casos más grandes y no de los más pequeños, que involucran pequeños montos. Por ejemplo, necesitan consolidar casos que afectan a muchas personas. Están sobrepasados. Trabajan muy duro pero la realidad es que no podemos depender de ellos ni contar con que nos proteja a todos porque es imposible.

En la Internet, las relaciones suelen regirse a través de un contrato. Si uno quiere tener un servicio como Google o Skype, hay términos de servicio para el celular, el servicio de cable, el ISP. Son contratos que nos estipulan los términos de servicio y que también le da a la parte el derecho de suspender el servicio, por ejemplo si se violan los términos de servicio. ¿Qué suele pasar? La gente en la industria de la seguridad o las víctimas hablan con el proveedor del servicio involucrado, llaman al

registrador o al registro y le dicen: “Está pasando algo mal acá. Tome alguna medida o llamen al proveedor del alojamiento y le dicen que hay un sitio que está haciendo phishing y que bajen la página”.

Hay un requerimiento de exigir el cumplimiento cooperativo para que se cumplan los términos de servicio mutuamente. La gente elige los servicios según los términos del servicio en un entorno competitivo. Mi opinión personal, y muchos en mi industria piensan lo mismo, es que cualquiera que opere un recurso en Internet tiene la responsabilidad de operar de manera inteligente, prudente, que tenga a las víctimas en cuenta. La Internet es una red de redes. Gran parte de las actividades en Internet carecen de órgano que las rija o las supervise. Hacemos lo mejor que podemos. La Internet es abierta, lo cual es fantástico, pero el ciberdelito es una de las desventajas de tener un sistema así de descentralizado. La siguiente.

Surge la pregunta de cuál es el rol que juega la ICANN en esto. Estas son mis reflexiones personales. Los estatutos estipulan algunas cosas genéricas sobre el ámbito que le corresponde a la ICANN, específicamente garantizar la operación estable y segura de los sistemas de identificadores unívocos de la Internet y políticas para las cuales sea necesaria razonablemente una resolución uniforme o coordinada para facilitar la apertura, etc. Por supuesto, ¿cuál es el alcance de todo esto? ¿Qué significa?

Una de las cosas que hace ICANN es acreditar a los registradores y los registros. Es decirles: “Usted tiene derecho de operar un registro y vender nombres de dominio gTLD”. Pero esto implica permiso. ICANN puede estipular políticas que se incorporan a los contratos a través de los procesos de la comunidad, etc.

ICANN otorga por ejemplo acceso a los datos de WHOIS y a los archivos de zona que son dos aspectos muy importantes para proteger a la gente. Estos datos pueden revelar mucha información acerca de qué está pasando en la infraestructura. Hay prohibiciones en los contratos contra el uso de los nombres maliciosamente y los registradores lo ponen en los contratos. Monitoreo de uso indebido para los registradores. Ahí están los registros.

Los contratos de la ICANN son ejecutables. Si no se cumplen las disposiciones, se pueden ejecutar. Hay que concentrarse en los grandes problemas. Como decía, gran parte de estas registraciones maliciosas se hacen en determinados lugares. Tenemos que entender por qué está sucediendo. Hay que promover la mejora en distintas maneras de esta situación. Con esto llego al final de mis diapositivas. Es momento de conversar.

ALAN GREENBERG: Eso espero. Andrei.

ANDREI KOLESNIKOV: Gracias, Greg. Creo que es muy importante decir que el uso indebido de los nombres de dominio es parte de una economía ciberdelictiva mucho más grande, que genera miles de millones de dólares. No son solo las personas que hacen uso indebido de los nombres o que se portan mal. Es un sistema que es una economía oscura, que gana miles de millones de dólares. Yo creo que tener herramientas en línea que ayuden a los registradores a tener los datos sobre el uso de los nombres de dominio supera lo que es gTLD. Es muy importante también para los ccTLD. Usted sabe que cuando yo estuve a cargo de .EU, hace muchos años, lanzamos esta buena herramienta en línea que permitía a la gente chequear los nombres de dominio. Los registradores pueden hacer un gran volumen de chequeos cuando reciben informes. Para hacer tal cosa, se requiere dinero, recursos.

Los grandes registros en los países o los gTLD pueden afrontar el costo de estas herramientas. Nosotros lo hicimos en nuestro caso sin propósito comercial, con fondos de las registraciones, con el registro nacional. ¿Cómo se organiza? Más allá de los servicios para los registradores y los registros que pueden usar este tipo de herramientas en línea, una carga de datos a granel. ¿Cuántos sistemas como este existen? Ya hace siete años desde que lanzamos este primer producto y ya perdí la cuenta. Un número aproximado.

ALAN GREENBERG: Si me permiten, tenemos unas siete personas en la fila de oradores. Puse el cronómetro pero no hay tiempo para restringir la respuesta.

GREG AARON: Hay distintas fuentes de datos que usan los registradores y los registradores. Algunos saben muy bien lo que pasa en sus espacios y algunos no. Debo decir que tienen que asignar un presupuesto para este tipo de medidas de información y mitigación, incorporarlo a los presupuestos. Si usted quiere datos, hay distintos lugares que le puedo indicar, donde la gente puede obtener acceso.

ALAN GREENBERG: Olivier.

OLIVIER CRÉPIN-LEBLOND: Este es uno de los temas. Yo soy el presidente de EURALO y este es uno de los temas que a mí me molestan mucho en ICANN y así ha sido desde hace años. Este tema precisamente es algo que perjudica a los usuarios finales. Es algo en lo que lamentablemente creo que ICANN no hace nada. ALAC consta que ha estado trabajando, buscando datos en los PIC sobre las

cadenas de caracteres para mejorar la seguridad, la verificación de los registratarios, etc. Esto fue descaradamente dejado de lado por las partes contratadas que querían vender al que fuera y querían el control sobre a quiénes podían vender.

Mientras tanto, yo hice mucha investigación y seguimiento de lo que hace el grupo de trabajo contra el phishing. Creo que a la mañana, por coincidencia, circulé un artículo que se refiere a su último informe, que muestra que esta situación no hace más que empeorar. Hace dos años, en 2015, cuando hablábamos con las partes contratadas sobre el uso de los nuevos gTLD para phishing y malware, etc. nos dijeron que eso no existía, que nada de eso estaba pasando. Nosotros sabíamos que iba a pasar. Ya estaba ocurriendo. ¿Qué podemos hacer al respecto?

Yo envié un mail a la lista del grupo de trabajo sobre los nuevos gTLD y pregunté si se podía incluir una disposición en los acuerdos con los registros para asegurar que se suspendan los sitios dentro de un plazo en los acuerdos de nivel de servicio. La gran mayoría suspenden los sitios rápidamente pero hay un pequeño grupo donde todos estos nombres son los malos y de un país específico que usted mencionó en el informe. ¿Qué podemos hacer al respecto?

GREG AARON: La mitigación es algo, como decía, a la que los registradores y los registros tienen que asignar una partida presupuestaria. A veces eso no pasa. La competencia en el espacio hoy día es muy intensa. En especial por el hecho de que los dominios se vendieron muy baratos. Nosotros vamos viendo que el uso indebido migra de un lugar a otro y eso depende del precio. Gran parte de estos dominios involucrados en delitos no son propietarios de una cadena de caracteres relacionados con la actividad. La mayoría de los dominios de phishing no tienen el nombre de la compañía. A los phishers no les interesa qué usar. Usan cualquier cosa.

Lo que me preocupa mucho es dónde se dan estos grandes lotes de dominios. Este es un problema de cumplimiento también. Tenemos herramientas que ya no sirven como el SLA de suspensión. Hay algunos desafíos en la creación de este tipo de cosas porque incluso los registradores más responsables y conocedores del tema pueden tener dificultades para cumplir con estas disposiciones. Creo que cumplimiento es una de las mejores herramientas que tenemos. Yo no sé si podemos aprovecharlo lo más posible.

OLIVIER CRÉPIN-LEBLOND: Tres palabras. Una tremenda vergüenza.

ALAN GREENBERG: Muy bien. Voy a usar un cronograma de un minuto y medio para el orador, con una alarma. Harold.

HAROLD ARCOS: Gracias. Voy a hablar en español. Gracias. Greg, gracias por la presentación. En esta oportunidad es oportuno lo que sucedió ayer a escala mundial para colocar sobre la mesa una pregunta que me han hecho varios usuarios en otras reuniones previas de ICANN. Ayer sucedió un ataque masivo. Uno que ya es el segundo después de WannaCry, en varios países que reportaron ataques como la India, Rusia, algunas empresas de Reino Unido. En otras oportunidades, los usuarios me preguntan qué hace ICANN en este respecto. Si es su responsabilidad colocar políticas dentro de los contratos que prevean esto.

En la presentación que nos acabas de hacer nos muestras que hay políticas para ello pero no hay un conocimiento preciso de qué sucede si no se cumple. Si no se cumple, no sucede nada. ¿Cómo en ICANN afrontamos lo que sucedió ayer? ¿Qué cosas puedes adelantarnos? ¿Qué se está haciendo? ¿Dónde se va a buscar la información? ¿O solo nos quedamos con la información del contrato? Gracias.

GREG AARON: El ataque se refiere a un ransomware. Es un ataque de malware. No he hecho una investigación con respecto a cuántos nombres de dominio fueron afectados pero estas son formas típicas de ataque. Una vez más, la mitigación se da de dos maneras. Por un lado, los registros reciben una llamada porque las compañías de seguridad las van a llamar. Hay información para ver si están monitoreando a los bloqueadores o a las listas negras. Algunas son comerciales, algunas son gratuitas. Se hace una lista de los nombres de dominio, y algunos registradores y registros utilizan estas listas para hacer un monitoreo. Pueden retirar los dominios en esos casos. Algunas de estas actividades son difíciles de detectar y están por todas partes. Se diseminan por todas partes. Lo que sucede con este tipo de actividades es que vamos a tener el cumplimiento de la ley finalmente, dado que son actividades masivas. Es a nivel internacional. Puede ser que les lleve tiempo a las agencias de cumplimiento de la ley proceder al respecto.

HAROLD ARCOS: Además de las agencias de seguridad, ¿ICANN dónde busca la información cuando sucede esto? Las agencias de seguridad tienen una tarea local, soberana, intrapaíses, ¿pero dónde acude a la información, dónde intervienen para hacer seguimiento?

GREG AARON: A veces el equipo de seguridad dentro de la ICANN obtiene información de fuentes externas. Especialmente si hay alguien que necesita ayuda para encontrar los contactos adecuados a quien dirigirse. Por ejemplo, puede haber un contacto en un registro y el personal de seguridad de la ICANN entonces puede facilitar este contacto. La ICANN también está comenzando a recibir y a consolidar datos sobre esto.

ALAN GREENBERG: El siguiente orador es Dave Piscitello.

DAVE PISCITELLO: Dave Piscitello, de ICANN. Soy parte del equipo de seguridad. Greg, uno de los comentarios se hizo sobre la amplificación de los nombres de dominio. Es decir, una gran cantidad de URL en un ataque de ese tipo. El nombre de dominio es un solo vector y en muchos casos solamente representa una fracción del ataque, no todo el ataque.

GREG AARON: Hay algunas cuestiones que se cumplen y hay muchas cosas que se pueden colocar en un nombre de dominio. Puede haber un subnombre de dominio o un subdirectorio. También pueden dividir el DNS para colocar sus propios nombres de dominios. Muchas veces hay muchos subdominios en diferentes partes. Un

nombre de dominio puede en realidad ser utilizado para perpetrar muchas actividades o diferentes ataques. Eso es importante tenerlo en cuenta.

También hay que tener en cuenta que algunos nombres de dominio dan apoyo a varios servicios y ciertas compañías están dedicadas a vender subnombres de dominios. Uno puede obtener un subnombre de dominio y no queremos retirar ese nombre de dominio principal porque hay muchos otros servicios que dependen de ese nombre de dominio principal. Por eso esos son los desafíos que tenemos al responder a este tipo de problemas porque no queremos causar más daño del que ya se ha causado.

ALAN GREENBERG: Tenemos dos oradores más. Kaili y Alberto, en ese orden. Por favor, les voy a pedir que sean muy breves porque nos estamos quedando sin tiempo. Vamos a tener que detenernos porque nos quedan dos tópicos más y muy interesantes para abordar.

KAILI KAN: Muchas gracias. Voy a ser breve, Alan. Formo parte del CCTRT el equipo de revisión del equipo sobre competición, elección y confianza de los consumidores. Esta mañana se habló sobre el abuso del DNS. Está el programa de los nuevos gTLD, que ya se

implementó hace unos años y quiero saber si esto tiene algún efecto o impacto en el uso indebido del DNS y también cuál es el debate actual con respecto a los procedimientos subsecuentes de los nuevos gTLD y si hay algo para prevenir el uso indebido del DNS, si hay algo que se pueda incluir en este proceso de política.

GREG AARON: Una pregunta que podemos hacer es si los nuevos TLD dan lugar a mayores delitos cibernéticos. También podemos preguntarnos si los nuevos TLD van a sufrir una migración de todas las actividades que ya se realizan.

KAILI KAN: Eso es lo que estoy preguntando.

GREG AARON: Vimos algunas pruebas de que los nuevos gTLD han atraído una parte significativa de este tipo de actividades. Vemos phishing y vemos spam. También comenzamos a medir estas situaciones. Lo que significa esto es que hay que trabajar con los operadores, los registradores y los registros, y hay que entender por qué sucede esto. Creo que una razón sería los precios bajos. Por otro lado, hay que preguntarse si los nuevos gTLD dan lugar a mayores delitos cibernéticos. Hay muchos nombres de dominios

para comprar en todos los gTLD y los ccTLD. Los delincuentes pueden obtener tantos nombres de dominio como deseen. No importa si están en un sector o en otro. Lo que hay que analizar es si el programa de los nuevos gTLD ayuda a los operadores y si se puede llegar a ellos o no.

ALAN GREENBERG: Tiene la palabra Alberto.

ALBERTO SOTO: Voy a hablar en español. Entiendo que ustedes deberían estar en coordinación con el GAC también. Me gustaría saber qué responde el GAC ante los avisos de ustedes respecto del posible mal uso de los dominios. Entiendo que el GAC, ya que ICANN no puede ir, pero sí cada país puede ir y tomar medidas dispositivas que sean realmente efectivas. No como hasta ahora.

GREG AARON: Gracias. Dentro del GAC hay algo que se llama grupo de trabajo de seguridad pública que se compone de funcionarios de cumplimiento de la ley y reguladores entre otros. Ellos asesoran al GAC respecto de qué asesoramiento el GAC le debería dar a la ICANN con respecto a los delitos cibernéticos y a las cuestiones de uso indebido de los nombres de dominio. Ellos le han pedido a la ICANN que implemente ciertas políticas como por ejemplo la

política de exactitud del WHOIS, que monitoree las políticas en relación a los usos indebidos. Están participando y ayudando al GAC a que le brinde asesoramiento a la ICANN. También llevan ese asesoramiento a los países locales, lo cual es importante.

ALBERTO SOTO: Mi pregunta es exactamente al revés. Entiendo que ustedes dicen "dentro de ICANN". Mi pregunta es: De vuestro grupo con el GAC y qué recomiendan ustedes que los respectivos gobiernos hagan, no ICANN.

GREG AARON: Una cosa que los países pueden hacer y que realmente ayudaría es implementar medios para que las autoridades de cumplimiento de la ley cooperen con intercambio de información con otras agencias de cumplimiento de la ley en otros países. Por supuesto, los delitos en Internet trascienden las fronteras y las agencias de cumplimiento de la ley tienen que poder hablar o conectarse con sus contrapartes en otros países. Para eso se necesitan leyes que les permitan hacer eso. Si no pueden hablar entre sí, si no pueden intercambiar información con facilidad, entonces tienen las manos atadas.

ALAN GREENBERG: Les agradezco a todos. Vamos a tener que finalizar esta sesión. Quiero agradecerle a Greg. Creo que ha sido muy informativa y también divertida. Gracias. Gracias a todos por las preguntas en la sala.

GREG AARON: Sé que se han quedado sin tiempo pero si tienen más preguntas, con gusto las voy a responder luego.

ALAN GREENBERG: Seguro nos vamos a volver a encontrar. Ahora vamos a contar con la presentación de Jonathan Zuck y los miembros del CCT. Los miembros del CCT pueden tomar asiento en torno a la mesa. Creo que no es necesaria mucha introducción para el tema. Hablamos de este tema con frecuencia y Kaili también nos ha dado informes al respecto. John, ¿quiere presentar a los otros colegas en la sala y contarnos qué está sucediendo? Sé que han tenido una semana interesante.

JONATHAN ZUCK: Muchas gracias, Alan. Gracias por darnos la oportunidad de hablarles sobre la competencia, la elección y la confianza de los consumidores. Soy Jonathan Zuck, presidente del CCTRT. También cuento con mis colegas, que trabajan en el tema de protección. Tenemos a Jordyn Buchanan, de Google, que trabaja

en el equipo de competencia y elección. También es el presidente de un subequipo que trabaja en cuestiones de aplicación y evaluación de la revisión.

Tuvimos una reunión presencial en la semana. Hablamos de una serie de cuestiones pero el foco se puso en dos o tres cuestiones. Una es el periodo de comentario que hemos recibido, lo que incluye uno del ALAC, y de qué manera abordarlos de mejor manera. Hay cuestiones generales que estamos planeando abordar en las próximas semanas. Los subequipos tienen que responder a estos comentarios a las recomendaciones. También teníamos una presentación sobre el informe interino del uso indebido del DNS. Con gusto les podemos contar al respecto. Drew está sentado allí. Él es el que lidera estas cuestiones del uso indebido del DNS. También podemos hablar de estos resultados. Vamos a emitir un informe para mediados de julio.

Finalmente, hemos hablado sobre una encuesta que hizo INTA. Algunos miembros de este grupo eran titulares de marcas comerciales. Hemos obtenido muy buenos resultados y aportes para nuestro trabajo. Otra cuestión que surgió de los comentarios de ALAC es el tema del parking o estacionamiento. También lo hemos debatido durante la reunión del fin de semana. No sé de qué manera proceder. No sé si Laureen me puede ayudar. Quizá ella pueda contarles sobre algunas cuestiones.

ALAN GREENBERG: Tenemos media hora. En teoría, nos quedan 20 minutos. Nos vamos a extender un poco pero no mucho porque tenemos otros oradores. Vamos a hablar del uso indebido de los nombres de dominio nuevamente. Perdón por interrumpir.

LAUREEN KAPIN: Voy a ser breve. Todavía estamos trabajando con los comentarios públicos que hemos recibido. Agradecemos todos los comentarios enviados desde ALAC. Nos han apoyado mucho en cuanto a las recomendaciones de la confianza y la elección de los consumidores. Lo agradecemos realmente. Compartimos sus inquietudes con respecto a la falta de fondos. También, en un mundo ideal, tendría que haber información sobre los niveles de confianza que tienen los consumidores en el DNS y en los nuevos gTLD en particular. Esperemos poder obtener mejor información como resultado de nuestras recomendaciones. También estamos trabajando hacia nuestro objetivo de redactar un informe final. Este proceso tiene un punto final y esperemos que sea la reunión de Abu Dabi.

Esto va a estar en su radar así que esperamos que haya más oportunidades de comentario público para las nuevas partes de nuestro informe y que estas partes nuevas del informe reflejen los resultados. Yo, en lo particular, no digo que sea lo más

importante, pero yo me he focalizado en el uso indebido del DNS y esperamos que el informe final de ese estudio incorpore los resultados de nuestro informe interino y las nuevas partes de este informe se van a publicar para comentario público. Me voy a detener aquí.

ALAN GREENBERG: Podemos decir que va a ser algo interesante.

JONATHAN ZUCK: Quisiera hablar un poco también sobre los resultados preliminares, sobre la encuesta de uso indebido del DNS. Creo que a partir de esta presentación vamos a comenzar a ver muchos estudios que van a tener resultados similares, vis a vis actividades de uso indebido en el DNS. Probablemente estos sean resultados promisorios para poder avanzar.

DREW BAGLEY: Gracias. Este es un muy buen momento para comenzar a hablar de este tipo de cuestiones.

GISELLA GRUBER: Por favor, quiero recordarles a todos que contamos con interpretación en francés, inglés, árabe y español. Por favor, les pido que se identifiquen cada vez que tomen la palabra para los

intérpretes y los participantes remotos los puedan identificar. Gracias.

DREW BAGLEY: Drew, del equipo de revisión de CCT. Ahora tenemos un informe preliminar. Hemos tenido más información pero hasta ahora lo que podemos ver es que lo más interesante para nuestro mandato tiene que ver con las tasas de uso indebido que se mantienen similares con respecto a la introducción de los nuevos gTLD y las registraciones siguen aumentando. La proporción se mantiene igual. Lo que parece suceder es que hay alguna sustitución en la cual la gente está pasando del uso de los gTLD legados al uso de los gTLD para ciertos tipos de uso indebido. Más allá de todas estas medidas de protección que abarcan a los nuevos gTLD, los resultados preliminares demuestran que no parece haber mayor prevención en el uso indebido de los nuevos gTLD pero, obviamente, vamos a tener más información cuando avancemos con el análisis.

Otra cuestión interesante a tener en cuenta es que hay tipos de uso indebido que prevalecen más en los nuevos gTLD, por ejemplo el spam. El spam prevalece más en los nuevos gTLD que en los gTLD legados. Parece que ha habido una migración. Quizá sea por la cuestión de los precios. Otra cuestión interesante es que los nuevos gTLD tienden a tener más nombres registrados

maliciosos que comprometen a los sitios web. Este es otro fenómeno que hemos identificado y sobre el que esperamos tener más información en los próximos meses.

ALAN GREENBERG: Muchas gracias. Vamos a dar lugar a las preguntas cuando finalicen los oradores.

JONATHAN ZUCK: El tema que nos queda, sé que es difícil recordar una pregunta en el anteúltimo día de la reunión, es el parking. Hay dos componentes. Uno es la contribución potencial, como mencionó usted y como nosotros dijimos en nuestros comentarios. El uso indebido del DNS y también la noción del parking como un indicador contrario del efecto competitivo de los gTLD. No sé, Jordyn, si quieres hablar un poquito del lado de competencia. Drew, del lado del uso indebido del DNS, del parking. En ambos es más una cuestión de falta de información, más que de demasiada información.

JORDYN BUCHANAN: Hemos hablado bastante de esto. En el comentario de ALAC ustedes señalaron que la tasa de parking en los nuevos gTLD es muy alta. En el rango del 60%. Va variando según el mes, dependiendo de lo que esté pasando, la metodología, etc. Está

aumentando la significancia. Está duplicándose el aumento. Primero tenemos que tratar de entender cómo se comparan las tasas con los heredados. Quiero ser correcto. Si pudiéramos encomendar datos con la misma metodología que usamos con los heredados para los nuevos, veríamos que la tasa para los heredados no sé si era de 48% pero era en los números más altos del 40%. Bastante alta pero no tan alta como con los nuevos gTLD.

Ahí dijimos: ¿Cómo justificamos este diferencial? Vimos dos perspectivas. En primer lugar, el efecto de la competencia. Luego, el efecto del uso indebido y la confianza del consumidor. En lo que hace a la competencia, está la hipótesis en el equipo de revisión de que posiblemente si hay muchos dominios estacionados no va a haber tanta renovación. Por eso los dominios estacionados pueden parecer hoy día populares pero a futuro quizá no sea una base estable para justificar nuestros hallazgos sobre la competencia. Trabajamos con las tasas de renovación para tratar de encontrar si había correlación entre las tasas de estacionamiento y las tasas de renovación. En nuestra prueba inicial, estamos en la fase de hipótesis todavía, no encontramos correlación entre ambas tasas.

En lo que hace a competencia, no entendemos todavía si existe alguna relación entre las tasas de estacionamiento y los efectos potenciales sobre la competencia. Tenemos otras hipótesis pero

por ahora debemos seguir testeando esta comparación. En lo que hace al consumidor, la confianza del consumidor, no está en el informe pero los autores nos han dicho que lo han evaluado. Hay una correlación blanda entre el equilibrio inferior de lo que es estadísticamente significativo entre sitios de parking que es un término más estrecho de lo que nosotros definimos como parking, que incluye también nombres sin servidores y con otros errores de términos más allá de lo que son las páginas de parking. Estas mismas páginas de parking, los TLD solían mostrar más uso indebido que otros TLD. No entendemos por qué. No sabemos si es el sitio o algún otro factor del TLD. Quizá son TLD muy baratos. En realidad no sabemos. Tenemos que hacer un análisis más profundo para saber cuáles son los vectores. Esperamos tener un componente del uso indebido del DNS cuando hagamos el informe final.

ALAN GREENBERG: Vamos a poner un temporizador de 90 segundos. La primera pregunta es de Holly.

HOLLY RAICHE: Quiero preguntar qué clase de uso indebido es más común con los nuevos gTLD. ¿Tienen alguna idea de por qué esto es posible, por qué está pasando? Gracias.

DREW BAGLEY: Gracias por la pregunta. Lo que hemos visto hasta ahora en el informe preliminar es que creo que hay dos tipos. Un tipo es spam, que está más presente en los nuevos gTLD que en los heredados. La manera en que se conduce el uso indebido, que es el segundo aspecto, ahí los datos muestran que las zonas de los nuevos gTLD tienen más nombres de dominio registrados para propósitos maliciosos. Mientras que el mismo tipo de uso indebido, ya sea phishing, alojamiento de malware o botnet en los heredados, lo más común es que sea de sitios web legítimos comprometidos. Tiene que ver con el alojamiento quizá o con el secuestro de los nombres de dominio y varias otras hipótesis. Esto es lo que marcan los datos preliminares. Todavía no sabemos por qué. Una teoría con la cual estamos operando es que quizá sea el precio, quizá hay aspectos especiales en los nuevos gTLD. Ofertas especiales.

HOLLY RAICHE: ¿Por qué dice “registrados”? ¿Se basa en evidencias?

DREW BAGLEY: Se basa en un modelo que los investigadores elaboraron, los que hicieron el informe sobre uso indebido del DNS. Ellos analizaron cuántos días le llevaba a un nombre de dominio comportarse

mal. Hay otras variables que se explican en el informe preliminar. La lectura seguramente le dará una mejor explicación de lo que yo recuerdo pero es una lista con un modelo basado en un estudio de hace unos años que halló este aspecto común entre nombres de dominio registrados por personas con mala intención, de hacer uso indebido del DNS.

ALAN GREENBERG: Una pregunta para Jordyn de mi parte. Si yo registro Hilton.hotels y me lleva a Hilton.com, ¿eso lo consideran parking e intentan medir qué porcentaje de los dominios estacionados están en la misma situación?

JORDYN BUCHANAN: Nosotros tenemos una definición muy expansiva de lo que es parking. Todo aquello que no tiene contenido directamente alojado en el dominio. Las páginas de parking y muchas otras cosas. Para responder su pregunta, sí, eso contaría como parking con nuestra metodología actual. Es un porcentaje relativamente menor de lo que entre comillas llamamos parking, que es el *redirect*, el 4%. No es la mayoría de los casos. Tengo a Satish.

SATISH BABU: Gracias. Quiero saber si hay evidencias de IDN susceptibles especialmente a usos maliciosos.

DREW BAGLEY: Para el informe preliminar no tenemos datos todavía, creo. Es un aspecto que sin duda nos interesa mucho porque no me sale el nombre pero hay estos ataques conocidos que buscan otros caracteres. No sé si tenemos datos. No sé si los investigadores pudieron evaluar estos casos. Le debo la respuesta y se la haré llegar.

ALAN GREENBERG: Olivier.

OLIVIER CRÉPIN-LEBLOND: Gracias. Perdón si voy a ser provocador ahora pero antes de ustedes nos visitó Greg Aaron del grupo antiphishing. Ellos recopilan muchos datos sobre estos temas. Ahora veo que siguen recopilando más datos. ¿Qué hace ICANN al respecto? Podemos tener todos estos datos, ¿pero estos datos van a ser usados para hacer algo? Actualmente, parece una tesis filosófica de la vida sexual de una pelota de pingpong. Es decir, son muchos datos pero para qué sirven.

ALAN GREENBERG: Quizá pueda reservar esa pregunta para alguien que sea de ICANN. Le voy a dejar a Drew que responda si quiere.

DREW BAGLEY: Nunca escapo a las preguntas provocadoras. Creo que lo que usted dice es algo que nos preocupa a todos en general. Gran parte de lo que hacemos en nuestras recomendaciones en general es convocar a que ICANN tenga un abordaje basado en las políticas. En especial con el estudio del uso indebido, es la primera vez que se hizo un estudio integral. Este análisis lo utiliza el APWG. Esta es la primera vez que se hizo un análisis integral histórico, que analizó cada una de las zonas. Mi intención era saber si podíamos medir que las medidas de protección puestas en práctica fueran efectivas o no. Si no lo eran, las percepciones y la confianza de los consumidores en los nuevos gTLD estaban o no en línea, si podían confiar en los gTLD nuevos más o menos que en los anteriores. En el informe final esperamos formular recomendaciones de políticas basados en datos. No es para nada una tesis filosófica sobre la vida sexual de una pelota de pingpong sino que es más una estrategia para jugar al pingpong.

LAUREEN KAPIN: Quería agregar, en una institución ideal, cuando se tengan datos específicos que correlacionen un tipo de conducta con un tipo de actividad, phishing o algún otro tipo de uso indebido, esto entrará al proceso de desarrollo de políticas. Por ejemplo, el GAC

podría usar esos datos y decir que tenemos que considerar la relación entre el precio y el uso indebido del DNS o quizá necesitamos disposiciones más estrictas en los contratos que hagan un monitoreo más rápido y efectivo del uso indebido del DNS y requiera respuestas. Estas son maneras concretas de usar estos datos para que no sea solo un ejercicio de recopilación de datos, que se ve muy bien pero cuando el agua llega a la puerta, importa aquí tener algún tipo de sanción.

JONATHAN ZUCK: Esta idea me suena bastante. Esta idea de la pelota de pingpong me va rebotando en el cerebro. Hay varios factores. Uno es el precio. Hay una expresión en inglés que es el tercer riel. Es el sistema de subterráneo que tiene un riel eléctrico que no se puede tocar. A veces esto es así en la comunidad ICANN. No se puede hablar del tema porque ICANN, de manera justificada, no se considera regulador de precios pero también vemos que hay una gran propensión en el área del spam, una gran presencia. El spam no es considerado en muchas jurisdicciones ilegal y no se define específicamente en los contratos como uso indebido del DNS. Nosotros lo vemos como la puerta de entrada al phishing. El spam, en ese sentido, es más difícil de evaluar.

Drew, corrígeme si me equivoco, pero si vemos las tablas que tiene el informe sobre uso indebido, las tablas muestran una

caída no importante pero una caída del phishing con los nuevos gTLD que quizá esté relacionada con la lista de medidas de protección, porque es una larga lista en los nuevos contratos. Empezamos a ver algunas prácticas específicas, algunos operadores de registros específicos que empiezan a mostrar menores índices de uso indebido, que son prácticas empíricas que deberían adoptarse de manera generalizada.

ALAN GREENBERG: El último orador es Sébastien Bachollet.

SÉBASTIEN BACHOLLET: Voy a hablar en inglés. ¿Han hecho algún tipo de comparación entre los datos recopilados?

JONATHAN ZUCK: ¿En qué aspecto?

SÉBASTIEN BACHOLLET: En cualquiera. ¿Tenían datos de las rondas previas? No sé si hay datos de las rondas previas. Si los hay, ¿hicieron alguna comparación con las rondas previas?

JORDYN BUCHANAN: Gracias, Sébastien. Depende del tema, creo. En general, sí hubo distintas acciones de recopilación de datos en las rondas previas. Ya lo hemos dicho. La ICANN no ha hecho acciones de recopilación robustas antes de esta revisión. En las rondas del 2000 y 2006 no hubo muchos datos que se recopilaran ni métricas en ICANN. No obstante, había estudios de terceros, comunidades académicas, en áreas en particular. En muchos casos sí recurrimos a esos estudios previos para tratar de entender la dinámica. La mayoría estaban orientados al área de la ecuación de la competencia, por ejemplo, algo que evaluamos es con qué rapidez crecían los TLD. .INFO, por ejemplo, en la ronda de 2000, cómo se comparaba con los nuevos gTLD. Me parece que no existen diferencias significativas de dinámica en lo que hace a la competencia con las rondas previas. Ha habido un gran cambio en el sentido de que ahora evaluamos un conjunto de TLD en su totalidad.

En el pasado lo que hacíamos era comparar .BIZ con .COM. Ahora nos centramos en ver como la colección completa de estos datos se compara con todos los gTLD. Eso representa las elecciones del consumidor. Así es como el consumidor hace la elección, no respecto a un único gTLD.

SÉBASTIEN BACHOLLET: Un agregado. Debo decir que, como yo estaba en aquella época, hubo acciones de recopilación de datos en la ronda del 2000. Cuando ustedes hablan de parking, por ejemplo, se hizo. El informe fue enviado a la ICANN pero nunca se publicó. Pienso que sería interesante tratar de encontrarlo. Si soy el único que sabe sobre este tema, quizá alguien de ICANN puede venir a preguntarme a mí.

ALAN GREENBERG: Gracias, Sébastien. Gracias, Jonathan y los demás. Vamos muy bien esta tarde por ahora con mis tiempos. Muy buena la sesión. Muchas gracias. Ahora tenemos a Dave Piscitello, quien hablará. En la agenda ven que él habla del TTFKAD, que se conocía como DART. Dave nos va a contar un poquito. No tenemos puntero láser. Perdón, nunca supe por qué.

DAVE PISCITELLO: Quiero presentarme. Soy Dave Piscitello, vicepresidente de seguridad y coordinación de TIC en ICANN. Mientras esperamos las diapositivas voy explicando la herramienta que antes se llamaba DART, que ahora se llama plataforma de reporte de actividad. Antes de venir a Johannesburgo recibí un correo del departamento de legales que decía que ICANN había recibido una carta de suspensión para el uso de DART como sigla porque

había otra organización que reclamaba el derecho de autor. Le cambiamos el nombre.

El proyecto a partir de ahora es proyecto de informes de actividades de uso indebido de nombres de dominio, que es el sistema DART. En sudafricano, se dice [inaudible], que quiere decir casa u hogar. Para evitar conflicto, espero que la próxima vez que nos veamos el nombre siga igual.

Les voy a explicar qué hicimos. Nosotros estamos creando una plataforma para reportar registración y uso indebido de nombres de dominio en los registradores y registros. Hace muchos años que hago esto, antes de empezar con ICANN. Estoy con ICANN desde hace 12 años. Ha habido grandes protestas e indignación acerca de la cantidad de uso indebido y muy pocos datos confiables. O vienen estos datos de fuentes comerciales, de fuentes limitadas o de la comunidad académica en áreas limitadas. Una de las cosas que decidimos hacer fue ser más abarcadores y lo más científicos posible. Estudiamos todos los registros y registradores de TLD para los cuales podemos recolectar datos de zonas y registraciones.

En este momento estamos estudiando 1.241 TLD. También fuimos a la bibliografía, leímos los informes comerciales. Fíjense que en la mayoría de los casos solo encontramos un número bajo de datos de proveedores en los estudios. Hay un gran

número de feeds de reputación, que después les voy a mostrar en la presentación cuáles son. Como sucede con la revisión del CCT, quisiéramos tener estudios históricos pero nuestros datos nos llevan para todos estos TLD al 1 de enero de 2017. A partir de ahora tendremos una gran base de datos para propósitos históricos. Obviamente, la recopilación de datos de los registradores de TLD va a ser más fácil que conseguir datos de reputación del pasado porque muchos proveedores no conservan esta información. Vamos a hacer un repositorio singular de datos de reputación.

También estamos estudiando múltiples amenazas. Son muy amplios estos estudios. Empezamos con el GAC. Identificamos en el comunicado original phishing, botnet y malware. No hacemos farming porque hay muy pocos temas de reputación o procesos que permitan la clasificación de farming. Es más un ataque que un uso indebido. Como nosotros creemos que spam es un aspecto importante del panorama, el GAC en Hyderabad tuvo una carta hacia la junta diciendo que las amenazas anteriores eran ejemplos y que les interesaba también el spam. Por eso nosotros incluimos el spam en nuestro estudio también.

Lo que intentamos hacer ahora es crear un conjunto de datos que no tenga sesgo y que pueda ser obtenido por cualquiera, y que utilice los mismos medios que otros utilizarían. Vamos a publicar un documento con la metodología. Lo que intentamos

hacer es recopilar prácticas científicas. Pensamos que si recopilamos lo que hacemos y lo que tenemos mediante una metodología, vamos a poder tener resultados similares a lo que ya hemos encontrado.

Quizá han oído hablar de la iniciativa de datos abiertos. Esta es otra actividad de la oficina de tecnología. Estamos intentando tener acceso a datos, a información y en cuanto a la pregunta qué vamos a hacer con los datos, bueno, esperamos poder publicar esa información. El proyecto utiliza únicamente datos que vienen de fuentes comerciales abiertas y públicas, como los datos de zona de DNS, datos de WHOIS. Utilizamos también datos de reputación de fuente abierta. En algunos casos se nos pide que paguemos una suscripción mensual para poder obtener nuestros feeds.

Una limitación o una desventaja con la que tenemos que lidiar es que tenemos datos que podemos utilizar de manera directa pero no de una manera para compartirla, porque no tenemos licencia para hacerlo. No lo vamos a poder hacer a menos que tengamos otro tipo de licencia. Siguiente diapositiva.

¿Cuáles son nuestros objetivos? Este no es un proyecto para que la gente nos diga: “Esto está mal. Esto está bien”. Hemos hablado con el GAC y la idea es identificar a quién hay que abordar, ya sea a la compañía de hosting, al registrador, al

registro. Saber qué acciones tomar para ver si es una acción que tiene que hacer cumplimiento de la ley o es una acción que se debe tomar en una sola jurisdicción, esto es algo en lo que estamos trabajando prácticamente a diario. Es una de mis labores diarias. No es un tema trivial ni un proceso trivial.

Lo que esperamos hacer con los datos es dar datos a la comunidad que den apoyo al proceso de desarrollo de políticas. Uno de los motivos por los cuales las políticas son importantes es para darle a la gente la posibilidad de tomar decisiones informadas. Hay proyectos de grandes datos que se están llevando a cabo. Los datos son importantes para tomar una decisión informada, ya sea sobre una política o sobre las consecuencias de una política o cómo resolver una situación. Este es el objetivo de esto.

¿Qué podemos hacer con los datos? Esperamos que podamos identificar las amenazas, informadas a nivel de TLD o a nivel de los registradores. Sería también bueno si en el futuro pudiésemos brindar listas de rastreo. Es decir, esto es algo que está dentro de nuestro alcance. También sería bueno poder rastrear las amenazas de seguridad porque con el tiempo esto fluctúa en el espacio. Uno puede tomar los TLD por un lado y hace 60 días había una cantidad de registraciones y este mes hay otra cantidad de registraciones. Esta es la forma en la que se manejan las registraciones. Varía. Lo mismo sucede con el spam.

Hay spam que está asociado a campañas masivas. Hay otro spam que está asociado a ataques. Estos datos tienen como objetivos ayudarlos.

Por supuesto, todo esto cambia en 365 días y la idea es poder darles una idea de lo que sucede y que tengamos datos para cada uno de los momentos o fechas y que uno pueda decir: "¿Qué sucedió en una fecha puntual?" Esperamos que esto dé una oportunidad para que el personal de la ICANN trabaje con la comunidad de la ICANN, especialmente con las partes contractuales para que consideren diferentes formas de administrar la reputación, los programas de uso indebido y también los términos del nivel de servicio.

Obviamente, las características más importantes de esto es estudiar la conducta maliciosa. Hay registraciones de nombres de dominio que se utilizan para propósitos maliciosos o delictivos. Es un problema muy serio para nosotros. Como mencionó Greg, parece que en el último año el registro de nombres de dominio que se utiliza para phishing se ha incrementado y hasta se ha triplicado. Esta es una inquietud. Queremos entender por qué está sucediendo. Siguiente diapositiva, por favor.

Ahora les voy a explicar de qué manera utilizamos los nombres de dominio y algunos datos. Recabamos los archivos de zonas de

los registros utilizando el servicio de datos de zona centralizada. Es una transferencia de zona. Tenemos aproximadamente 195 millones de nombres de dominio que tenemos en este momento y 1.241 TLD.

Actualmente, nos hemos contactado con algunos ccTLD. Yo estuve en la presentación que se hizo en el simposio de ccTLD. Debatimos con ellos todo esto. Esta semana, en la ccNSO sé que habrá más presentaciones. Sería bueno que todos pudieran participar porque les van a dar un panorama muy valedero de lo que sucede en el espacio. Siguiente diapositiva.

Utilizamos el WHOIS y, afortunadamente, para nosotros tenemos el DART, porque lo único que utilizamos del WHOIS son los datos de registración publicados. Esto es para un porfolio, para un perfil. Los puntos de contacto o ese tipo de datos no es importante para nosotros. Nosotros utilizamos la fecha de creación y de expiración para hacer otro tipo de análisis y el tiempo mínimo que un nombre por ejemplo con fines maliciosos permanece activo, cuándo se observó por primera vez el nombre de dominio dentro del DNS, pero no necesitamos más información relacionada con información personal.

En el porfolio de los registros utilizamos cierta información. Nuestra filosofía es que las amenazas de seguridad se pueden ejecutar incluso si un nombre de dominio no puede resolver una

dirección de IP. Utilizamos varios conjuntos de datos. Pasamos mucho tiempo en este proyecto tratando de decidir qué conjunto de datos en relación a las amenazas utilizaríamos e incorporaríamos. Tenemos 20 conjuntos de datos de 20 proveedores de datos de reputación. Les puedo contar cuántos artículos académicos e informes comerciales hemos analizado. Hemos hablado con los proveedores, con quienes venden los datos para poder entender la metodología y las prácticas que tienen.

Greg Aaron y yo trabajamos en esto. Hemos elegido una lista que tiene cobertura global y tasas de falsos positivos. Lo que queremos hacer con este proyecto es lo siguiente. Estamos tratando de ver cuáles son los usos que hacen los usuarios o las empresas y analizar las medidas de defensa o sistemas de seguridad que utilizan para evitar el spam y todo el malware. Una vez que tengamos todos esos datos los vamos a poner en un repositorio. Trataremos de que nuestra comunidad vea cómo otras comunidades externas a la ICANN ven estos sistemas. Esperamos que este proyecto sea extensible. Esperamos también que se puedan agregar nuevos datos conforme pensemos que es confiable. Por ejemplo, si en algún momento en el futuro hay información que es menos relevante o menos precisa, podemos por ejemplo considerar la posibilidad de retirarla. Hay circunstancias en las cuales históricamente una

lista ha comenzado como un proyecto de investigación. Tuvo cierta financiación pero después el proyecto se estanca. La reputación de la lista se reduce de esa manera. Por eso no queremos que esto suceda. Siguiente diapositiva.

También quiero que quede claro que la ICANN ahora no está investigando phishing o spam. Estamos utilizando la información que nos dan los proveedores de datos de reputación. Utilizamos información de nombres de dominio y de uso indebido. También confiamos en estos proveedores de información. Podemos manejar una serie de contadores. Por ejemplo, las amenazas de seguridad las hemos clasificado en cuatro categorías que ya mencioné: spam, phishing, el hosting de malware y botnets. También tenemos un total de nombres de dominio identificados desde el día uno. La idea es llegar al punto en que tengamos años de información. También hemos creado histogramas, cuadros para los diferentes TLD en comparación con los TLD legados y los ccTLD entre otros.

Cuando nosotros contamos un nombre de dominio, duplicamos. Obviamente, cuando utilizamos varias listas hay casos en los cuales vemos un nombre de dominio que está enumerado dos veces pero solamente lo vamos a considerar una sola vez. Consideramos que tenemos un conjunto bastante extenso y preciso de dominios. Este es nuestro conjunto de datos de reputación actual. Es una lista extensa. No aparece la totalidad.

Hemos elegido esta lista para garantizar que al menos tengamos dos listas para la clasificación de amenazas. Las elegimos porque soportan los mecanismos de verificación que nosotros buscamos.

También hubo mucha curiosidad y en algunos casos inquietudes sobre por qué utilizábamos varios conjuntos de datos, porque esto daba lugar a la duplicación. En cuanto a continuar con la investigación y al hablar con algunas personas que también habían realizado investigaciones en relación a las listas de bloqueo, en realidad nos dimos cuenta de que hay listas que a veces se superponen entre sí. No siempre, porque las metodologías son diferentes. Las redes de recabación de datos varían. Algunas son similares pero operan de manera diferente a nivel regional. Hay diferentes asociaciones con diferentes proveedores de servicios de Internet. Tenemos confianza en que podemos utilizar múltiples listas.

Comenzamos con una lista de 86 listas. Con Greg hicimos una serie de ensayos o pruebas con los TLD. Nuestros resultados confirman lo que el documento de Metcalf y Spring muestra. Esto representa un punto positivo para la claridad porque cuando comenzamos a hablar de una adopción de un sistema de seguridad, casi hubo una adopción consensuada del sistema que utilizamos. También estamos tratando de evaluar la calidad sobre la base de otros principios como por ejemplo literatura

académica. Voy a abordar esto rápidamente porque quiero que tengamos tiempo para interactuar.

No tenemos toda la información pero sí la suficiente para realizar evaluaciones exactas. En cuanto a los conteos que tenemos, lo que estamos experimentando es alguna forma de medir los grandes TLD en comparación con los pequeños TLD. Tenemos un porcentaje simple de uso indebido. Es una fuente métrica. Vamos a pedir que la comunidad nos brinde sus aportes con respecto a todas estas métricas. Esto es parte, por supuesto, de todo el proceso de debate que vamos a tener con usted y que se va a llevar a cabo esta semana.

El porcentaje de uso indebido y su cálculo es bastante sencillo. Es una fracción. Es el número de nombres de dominio que están en la lista de uso indebido en un TLD en un día dado dividido entre el número de dominios en la zona de TLD multiplicado por 100. El porcentaje para calcular el uso indebido en los registradores es el mismo. Esto se divide por el número de dominios patrocinados.

Les voy a mostrar lo siguiente. Estos son algunos de los ejemplos o la forma en la cual visualizamos los datos. Este gráfico muestra el porcentaje de uso indebido. Phishing y spam parecen estar migrando desde los TLD o parecen distribuirse entre todos los TLD de manera uniforme en tanto que el hosting de malware y

botnet permanecen mayormente en los TLD legados. Este es obviamente el gráfico de un solo día. Creo que falta una diapositiva.

Este es uno de los datos más interesantes que pudimos obtener y que logramos explorar. Cada uno de los diamantes que ven en el gráfico representa un TLD. Todos están en escala porque tenemos mucha congestión en cuanto a la representación gráfica pero la línea que cruza el gráfico de 0.6 es el porcentaje medio de uso indebido y, como pueden ver, hay una gran cantidad de TLD legados y nuevos que funcionan muy bien. Lo que no se muestra en esta diapositiva es que desde el 31 de mayo solo 365 de todos los TLD tuvieron más incidentes. Hubo otros TLD que no presentaron incidentes en absoluto.

Nuestro punto de preocupación tiene que ver con el eje que dice 10, porque hay aproximadamente 25 TLD que tienen un alto porcentaje de uso indebido. De hecho, tienen la mayor parte de actividades o registraciones maliciosas o informes de uso indebido del DNS dentro del sistema DART. Una de las interpretaciones que hicimos de esto es por qué esto sucede. Qué es lo que hay que hacer como comunidad para poder disminuir los porcentajes de uso indebido en lo posible a cero. Siguiente diapositiva.

Esta es la última diapositiva. ¿Cuál es el estado del proceso? Nos encontramos en la fase beta. Tenemos mucha dificultad en obtener datos del WHOIS. Hemos tomado en cuenta diferentes fuentes de datos para poder avanzar a un ritmo sostenido, incluida la del WHOIS. Creemos que los operadores de cc se unan a nuestro trabajo. La idea es que la comunidad nos diga de qué manera quiere que informemos esta información. Es decir, qué tipo de representación o qué tipo de datos quieren que nosotros les brindemos, hacia quién tenemos que dirigir esta información y qué tipo de acceso a los datos deberíamos considerar. Voy a detenerme aquí y voy a tomar las preguntas que tengan. Gracias.

ALAN GREENBERG: Tendré que irme en un momento. Si Olivier o Cheryl pueden ocuparse de presidir la sesión. Voy a hacer una pregunta breve. Luego Alberto y Garth. Le voy a pedir después a Olivier que se ocupe pero podemos seguir durante el receso. ¿Podemos ir a la diapositiva anterior? Usted dijo que no están en el negocio de cambiar los nombres pero veo que es un registro que indica casi un 100%. ¿Vamos a tener acceso rápido a los datos para saber de quién se trata? Usted quizá no, pero nosotros sí.

DAVE PISCITELLO: Es una pregunta que tiene que hacerse la comunidad. Yo soy una base de datos. Soy una base de datos para ustedes. Lo que la

comunidad de ICANN puede hacer es decidir cómo representar estos datos y en qué forma. Nosotros tenemos que tomar asiento y entender cómo hacerlo porque no tenemos una interfaz de usuario que alguien pueda entrar y escribir y obtener los datos que quieran. Tenemos que generar un sistema de información de datos y, para eso, tenemos que tener una idea de la comunidad de qué clase de informes quieren que produzcamos. Por eso estamos en beta.

Aliento a ALAC a que haga lo mismo que hicieron los otros grupos cuando nos reunimos con ellos. Hay algunas ideas. Lo van a pasar al GAC. El GAC lo va a presentar a la junta. Les sugiero que hagan lo mismo. Si ustedes quieren algún cambio, tienen que justificarlo. Les doy los datos y ustedes generan las listas. Si quieren alguna otra cosa, algunos de los jugadores que son más criticados por información anecdótica, son quizá los mejores operadores en el campo. Los mejores 25 TLD, por ejemplo.

ALAN GREENBERG: Gracias. Tenemos a Alberto, a Garth y a Holly. Me tengo que ir y me dijeron que las intérpretes nos dan cinco minutos. Podemos seguir más tiempo pero solo en inglés.

OLIVIER CRÉPIN-LEBLOND: El que sigue es Alberto Soto. Voy a hablar en español. Sé que este tema es hipercomplejo. Lo hemos visto con las exposiciones anteriores. Es tan complejo como cuidar a la abuela para que no se muera. Sucede que muchas unidades constitutivas le piden a ICANN que cuide a la abuela para que no se muera pero esa misma unidad constitutiva quizá es la que le tiene que tomar la fiebre. Cuando se muere la abuela, ICANN tiene la culpa. Mi pregunta concreta sería: ¿Qué dijo que iba a hacer el GAC respecto del primer objetivo de este proyecto que es la identificación? Evidentemente, ICANN solo no puede trabajar en esto y algún compromiso debería tener el GAC para poder hacerlo también.

DAVE PISCITELLO: Gracias. No voy a hablar en nombre del GAC. Lo que yo le he reportado, lo que yo presenté, fue esta información al grupo de seguridad pública. Ellos mostraron un gran entusiasmo por las oportunidades que representaban estos datos, estos conjuntos de datos. Ellos van a revisar el tema juntos, van a elaborar una lista de recomendaciones para el GAC y el GAC va a ir a la junta con lo que se derive de esa lista, con lo que ellos consideren que es apropiado para consideración de la comunidad y de la junta. No sé qué va a hacer el GAC porque, al igual que usted, yo solo le presenté el tema a comienzos de la semana. Yo tengo optimismo

de que con el entusiasmo demostrado vamos a poder hacer algún tipo de informe significativo.

OLIVIER CRÉPIN-LEBLOND: Gracias, Dave. Yo tengo una lista que me dio mi predecesor. Garth, Holly, Harold Arcos, Ricardo Holmquist. No sé si hay más tiempo. No, Holly no. Garth, usted sigue en la lista. Luego Harold, ¿usted quiere seguir en la lista o puede hablar con Dave Piscitello después? Ricardo, ¿puede hablar con Dave directamente después? Es por los intérpretes, que no han tenido un receso. Si les parece, vamos a Garth Bruen.

GARTH BRUEN: Garth Bruen, de ALAC América del Norte. Me hago eco de lo que dijo Olivier antes, que ha habido mucho ruido y muy poca acción. Obviamente algo tiene que estudiarse antes de ser encarado y no hay duda, Dave, de que sus datos, sus resultados van a ser específicos y exactos. No hay dudas al respecto. Tengo mucha fe en usted. El tema está en el seguimiento. Qué va a pasar a partir de ahora. Supongamos por un minuto que hay un proceso de cumplimiento efectivo basado en lo que dijo Greg, lo que dijo usted y lo que dijeron otros. Algunas de las cosas que quizá cambien es que quizá suban los precios, que un gran número de dominios puedan ser removidos del DNS porque son abusivos, que haya que crear mecanismos para exigir el

cumplimiento. Todas estas cosas van a reducir las ganancias netas de ICANN. ¿Cuál es el incentivo que tiene ICANN para hacer cualquiera de estas cosas?

DAVE PISCITELLO: Yo vengo del mundo de los dominios desde hace 15 años pero fui una de las primeras personas que compró un dominio .COM, por el cual pagué 50 dólares hace mucho tiempo. Antes de hablar de aumentar los precios yo creo que si la industria dice que cualquier dominio para cualquiera cuesta 40 o 50 dólares, no existirían tantos dominios si todos pagamos lo mismo. Otra cosa, no quiero entrar a hablar de precios pero lo estamos evaluando y esperamos establecer alguna correlación entre los nombres y los precios para Abu Dabi. Esa es una de mis próximas metas. Creo que es prematuro hacer presunciones de que los ingresos de la comunidad de la ICANN van a crecer por liberarse del abuso, porque no es así.

El uso indebido ha estado aquí desde que existen los nombres atractivos. Si por algún lugar hacemos que las cucarachas salgan corriendo, las cucarachas no van a desaparecer. Vamos a tener el mismo problema, aproximadamente la misma cantidad de uso indebido. Como decía Greg, en realidad no vemos que haya un incremento significativo. Vemos que hay un desplazamiento. Mis datos lo que me indican es que no solo hay mucho

desplazamiento sino que hay mucha gente que está dando vuelta y saboreando, probando, pasando de un TLD al otro.

Como anécdota les puedo contar que los que alojaban 100 dominios, ahora solo tienen 50. ¿Por qué? Porque se pierde el interés. Es muchísima la información y la inteligencia que podemos aplicar en el futuro cuando tengamos estos datos. Usted mismo también tendrá más conocimiento de las contramedidas que podremos implementar contras estas cosas pero, por primera vez desde hace 12 años, tengo la confianza de que tendremos los datos para avanzar y para hacer algo realmente significativo para poder manejar el uso indebido.

OLIVIER CRÉPIN-LEBLOND: Muchas gracias, Dave, por venir aquí. Tuvimos una hora y media de grandes programas de recopilación de datos pero parece ser que los datos no se ven tan bien para los usuarios finales. De todas maneras, gracias a los intérpretes por haber extendido su horario y a todos los demás. Hay otras sesiones en otras salas a las cuales son invitados. Buenas tardes a todos. Se levanta la sesión.

[FIN DE LA TRANSCRIPCIÓN]