YEŞIM NAZLAR: Buenos días, buenas tardes, buenas noches a todos. Bienvenidos a esta llamada que corresponde al webinar de creación de capacidades de At-Large sobre el uso indebido del DNS desde una perspectiva del usuario final en el lunes 4 de mayo de 2020 a las 15:00 UTC. No vamos a estar tomando la asistencia de todos los participantes porque hay muchos pero ustedes podrán encontrar la lista en la página wiki. Les queremos recordar a todos los participantes que están conectados por vía telefónica por la sala de Zoom que por favor silencien sus líneas cuando no están haciendo uso de la palabra para evitar interferencias y ruidos. Por favor, digan su nombre también cuando estén haciendo uso de la palabra, no solamente para los fines de la transcripción sino también para permitir una interpretación correcta. Por favor, mantengan silenciados sus micrófonos hasta que lleguemos a la sesión de preguntas y respuestas. Si ustedes levantan la mano, el moderador les va a dar el uso de la palabra y recuerden conectarse por la ventana del chat con los otros participantes. Por favor, asegúrense de utilizar todas estas funciones. Tenemos interpretación en inglés, español y francés y también transcripción en tiempo real. Van a encontrar el enlace a la transcripción en la ventana del chat. Muchísimas gracias a todos por participar. Ahora quisiera darle la palabra a Joanna Kulesza, copresidenta del grupo de trabajo de creación de capacidades de At-Large. Le doy la palabra, Joanna.

JOANNA KULESZA: Muchísimas gracias, Yeşim. Bienvenidos al segundo webinar del grupo de creación de capacidad de At-Large. En este momento les vamos a dar

información actualizada sobre el uso indebido del DNS y luego vamos a tener una sesión de preguntas y respuestas sobre este tema de tanto interés, sobre todo en el contexto de la pandemia porque también esta pandemia ha sido utilizada para el uso indebido del DNS. Muchísimas gracias a todos por organizar este seminario web como parte de la serie de webinars de nuestro grupo. Gracias a Jonathan también por aceptar la invitación para conducir este webinar y muchísimas gracias a Drew también por sumarse a nosotros y darnos información actualizada sobre el uso indebido del DNS y sobre algunos puntos específicos en estos momentos tan especiales.

Este año hemos armado un formato diferente. Tenemos los oradores en pantalla con información de parte de ellos y a ellos les va a interesar también conocer su devolución. Por eso tendremos una sesión de preguntas y respuestas. Ahora sin más quisiera darle la palabra a Jonathan y a nuestros invitados para comenzar con este seminario web. Muchísimas gracias, Jonathan. Le damos la palabra.

JONATHAN ZUCK: Muchísimas gracias, Joanna, por la invitación. Muchas gracias a todos por participar. He presentado un vídeo que es bastante breve. Espero que lo disfruten. Quedo a su disposición para las preguntas al final. Buenos días, buenas tardes y buenas noches para los que no son tan afortunados y es mitad de la noche. Hoy vamos a hablar del uso indebido del DNS que ha sido utilizado también en la crisis de la COVID-19. Escuchamos mucho del término ciberdelincuencia pero qué es el uso indebido del DNS. Todos estamos muy familiarizados con el sistema de nombres de dominio, el DNS. Nos presenta una serie de preguntas y

respuestas que pasan por toda la web. Es como una cacería donde necesitamos una persona que nos dé los datos de otra persona que a su vez nos informe sobre otra persona para poder llegar a aquella que queremos alcanzar. Es importante hacerles las preguntas a las personas correctas.

Como Dorothy, que fue la que tuvo que hacer las preguntas para llegar al Mago de Oz. Hablamos del uso indebido del DNS como un uso delictivo del DNS. Algunas personas tratan de dividir esta definición hablando de un uso indebido del DNS, ataques sobre el DNS y ataques utilizando el DNS o un uso incorrecto del DNS. Nosotros lo vamos a llamar en términos generales uso indebido del DNS.

¿Qué es ese sonido? Bueno, es una alarma. La primera pregunta es qué es el DNS. Es la Sociedad de la Naturaleza de la UEA, la División de Seguridad Nuclear o el Sistema de Nombres de Dominio. Esta alarma era para que ustedes respondieran. Si ustedes eligieron C, el Sistema de Nombres de Dominio, van a estar en lo cierto. La sociedad de la naturaleza de la UEA y la División de Seguridad Nuclear son DNS pero no del tipo del que hablamos aquí.

Hay que pensar también que aquí un criminal utiliza computadoras para hacer varias conexiones y abrumar el sistema. A veces hay un elemento criminal que se interpone entre usted y los servidores de los cuales está solicitando la información. Esto es un ataque con el hombre en el medio o un envenenamiento de la caché del DNS. Simplemente la idea es que las consultas son interceptadas y uno recibe el número incorrecto para el sitio que quiere visitar. Esto puede ocasionar un redireccionamiento. Algo que se llama un ataque de farming. Algo que sería como un

phishing, una suplantación de identidad, sin un atractivo que lo lleve allí. Uno piensa que está ingresando al sitio que le interesa pero en realidad está dando todas sus credenciales para el banco, por ejemplo, para que los delincuentes puedan acceder a sus datos reales en el sitio real del banco.

Uno de los abusos más comunes del DNS es el phishing, la suplantación de identidad. En ese caso se recibe un correo electrónico que sugiere algo que ha ocurrido con su cuenta bancaria y ustedes tienen que ingresar para corregirlo. Este proceso se llama phishing, suplantación de identidad, porque a uno lo engañan para ingresar a un sitio fraudulento. Fíjense. Este es un ejemplo de lo que podría decir ese email. Ustedes pueden ver aquí algunos elementos clave para estos correos. En algún momento de crisis con poco tiempo para corregir las cosas. Uno no piensa demasiado y se conecta a la cuenta. Por supuesto, está yendo a un sitio fraudulento y solamente con el uso de estos correos. A veces tienen también adjuntos.

Algo que es muy importante para At-Large son los IDN, el sistema de nombres de dominio internacionalizados. Estos nombres de dominio utilizan caracteres que no son latinos. Hay dominios relativamente nuevos que son esenciales para llegar a los próximos 4.000 millones de usuarios en Internet. El 70% del mundo utiliza alfabetos que no son de origen latino. En el 2012 pudimos registrar nombres de dominio en otros idiomas. Por supuesto, con la innovación también vienen los delincuentes con innovaciones. Los IDN no quedan al margen de esto. Resulta que hay muchas letras que no son del alfabeto latino que se parecen a las letras del alfabeto latino. Quién iba a imaginar de cuántas

maneras distintas se podía deletrear Bank of America. Cuando alguien ve estas palabras, uno lee el email rápidamente.

Otra vez la alarma. Vamos a ver esta pregunta ahora. ¿Qué es un ataque con denegación de servicio? Cuando una camarera está molesta contigo, cuando hay demasiadas solicitudes de un servidor web o cuando estamos llegando a la tienda sin zapatos. Es cierto. Es la respuesta B. Demasiadas solicitudes de un servidor web. Es cierto que entrar a un negocio sin zapatos puede llevar a una denegación de servicio pero en este caso es usted el que induce ese ataque.

Además de recolectar las credenciales, aquí hay un objetivo principal que es el de utilizar un software en una máquina que puede ser un software malicioso pero también puede ser de otro tipo. Ustedes habrán escuchado hablar de este tipo de programas, les habrán afectado a ustedes o a su familia. No tenemos tiempo para entrar en todos los detalles pero cuando uno habla de spyware o de ransomware no lo quiere tener en su computadora. Lamentablemente, las infecciones por software malicioso están aumentando. En los últimos 10 años han aumentado un 700%. A modo de ejemplo tenemos los ataques donde se pide un rescate, el ransomware, que han aumentado en 350% solamente en el 2018.

Para ser justos, después de la revisión de la ronda del 2012 de los TLD para los fines de la competencia, la elección y la confianza de los consumidores quienes trabajan en el departamento de cumplimiento contractual de la ICANN empezaron a hacer sus mejores esfuerzos y comenzaron a publicar datos más granulares sobre estos reclamos pero esto todavía no alcanza.

Ustedes habrán escuchado hablar del informe de actividad de uso indebido de los dominios, DAAR, que la ICANN comenzó a utilizar hace unos años. Hay informes mensuales que les dan suficientes datos para saber cuál es el problema pero no les dan suficiente información como para evitar que un dominio o un registrador que no parece ser bueno siga avanzando. Sin embargo, estos informes han permitido detectar varios casos pero todos estamos de acuerdo en que el uso indebido es un grave problema para los usuarios individuales.

¿Qué podemos hacer en At-Large? En At-Large podemos tener un abordaje por dos frentes para combatir el uso indebido del DNS. A través de la difusión de información y del desarrollo de políticas de la ICANN. At-Large va a desarrollar materiales educativos para los usuarios finales para protegerlos del uso indebido del DNS. At-Large es único en su estructura porque hace posible distribuir información a las organizaciones regionales de At-Large o RALO, quienes a su vez pueden distribuir esos materiales a sus estructuras At-Large. Cada una de ellas tiene miembros individuales que pueden terminar distribuyendo estos materiales.

At-Large ha estado desarrollando esta red durante años para poder llegar a los usuarios y protegerlos de los criminales que están en Internet. Hay distintos mensajes que pueden ser entregados para evitar que estas personas caigan en estas trampas todos los días. La verdad es que los delincuentes obtienen la mayor información que necesitan de los usuarios no siendo ingenieros sumamente inteligentes sino buenos ingenieros sociales. Si uno les da la contraseña, básicamente les abre las puertas y At-Large necesita educar a los usuarios para que estén atentos para ver esas noticias y detectar aquellas que son o demasiado buenas o

demasiado malas. Siempre hay maneras de descifrar si un correo electrónico es fraudulento o no. Nosotros nos reímos a veces de los correos electrónicos de phishing porque tienen una mala gramática pero no nos damos cuenta de que esa mala gramática es intencional. Escribir las cosas de esta manera dispara una eliminación de aquellos que reconocen este engaño y genera una empatía en aquellos que son menos sofisticados. At-Large puede ayudar a los usuarios a discernir cuáles son auténticos y cuáles no lo son.

Es importante también resaltar que los usuarios finales tienen que tener un software de protección contra los virus en sus dispositivos y en sus computadoras. En Estados Unidos nosotros esperaríamos una sofisticación considerable por parte de los usuarios. Casi un 50% de las computadoras sin embargo carecen de protección antivirus. At-Large debe alentar a los usuarios finales a que les pidan a sus empleadores que tengan servidores compatibles con DNSSEC para evitar este tipo de ataques.

Hay otro lugar donde necesitamos hablar de esta protección y es en los corredores, en las reuniones y en las llamadas en conferencia del proceso de desarrollo de políticas de la ICANN. A veces una llamada en un corredor o una participación en un grupo de trabajo puede ser el punto de partida. Tenemos que trabajar para lograr reformas, tanto dentro de la ICANN como entre las empresas que utilizan sus servicios para atender a los usuarios finales como los registradores y los registros. En otras palabras, si alguien habla del clima, nosotros podemos tender nuestra mano, mirar al cielo y decir: “Sí, esto me parece que es un uso indebido del DNS”.

Por suerte no estamos solos. Gran parte de la comunidad de la ICANN está preocupada por este tema y no quiere pasar a una nueva ronda sin una reforma significativa. No hay manera de que una minoría de voces puedan llegar a una ronda de la ICANN nueva sin tener el apoyo del resto de la comunidad. At-Large tiene que seguir trabajando con otros grupos para poder hacer sonar las alarmas y promover de manera activa la reforma. Nuestra primera tarea es mantener la línea abierta. No tiene que haber una ronda nueva hasta que se haya tratado de manera valiosa el problema del uso indebido del DNS. Para el departamento de cumplimiento es necesario tener una visión holística en su conjunto del uso indebido del DNS. No podemos simplemente reaccionar ante los reclamos y denuncias. Tenemos que usar nuestro poder de auditoría para reconocer los altos porcentajes de uso indebido y tomar acciones. Los registros y los registradores son parte del problema. At-Large va a seguir defendiendo una mayor fricción para esta actividad, para requerir autenticación de los registratarios porque hay una alta correlación con el uso indebido del DNS y el volumen. El equipo de revisión de CCT y el equipo de revisión de seguridad y estabilidad han sugerido que el diseño de la ICANN tenga incentivos para adoptar mejores prácticas. Ciertamente se está haciendo más investigación según las recomendaciones de los equipos de revisión del ALAC y ahora de VeriSign. Hay esencialmente 20 millones de dólares más en el presupuesto para invertir en seguridad y estabilidad del DNS.

Ciertamente hay registros y registradores que están invirtiendo un tiempo y un dinero significativo en combatir el uso indebido. De hecho, hay 48 empresas que se han sumado a un compromiso para aplicar las mejores prácticas. Eso es maravilloso pero igual necesitamos reformas

para abordar a los malos actores y francamente incluso los buenos podrían estar mejorando sus trabajos, poniéndoles las cosas difíciles a quienes no las hacen bien. Este es un recordatorio, esta caricatura que vemos, de que hay algo que se llama “las mejores prácticas” pero estas mejores prácticas a veces se transforman en algo normal y ya no siguen siendo las mejores. Los criminales no están satisfechos con el statu quo y nosotros tampoco nos podemos dar el lujo de estarlo. Los buenos siempre pueden mejorar.

Se está haciendo muchísimas investigación ahora en el aprendizaje automática de máquinas para detectar los usos indebidos en tiempo real y para predecir si se pretende utilizar una registración de manera ilegal. Hay pruebas tempranas de la tecnología por parte de .EU que muestran una exactitud de casi el 80% en estas predicciones. Tenemos que asegurarnos de que continúe la investigación y los sistemas para protegernos de la próxima generación de ataques.

Parece que es tiempo de responder otra pregunta. ¿Cuáles son las mejores herramientas para combatir el abuso del DNS? La educación, el DNSSEC o la encriptación de extremo a extremo. Si ustedes eligieron todas, tienen razón. Si no lo hicieron, por favor, quédense después de la hora.

Habiendo dicho todo esto, solamente hay una unidad constitutiva de usuarios finales. Con los intereses de los usuarios finales en mente fue creada At-Large. El uso indebido del DNS los afecta a todos. Nosotros no podemos hacer un uso del uso indebido del DNS. Ustedes pueden entrar a nuestra página wiki que ven aquí en pantalla para tener más información. Gracias. Gracias a todos. Si tienen alguna pregunta en este

momento antes de pasarle la palabra a Drew. Viendo que no hay preguntas, ¿el personal ha visto alguna pregunta en el chat? Yo no veo ninguna. ¿Hay una pregunta en el chat? Adelante.

YEŞIM NAZLAR: Estaba por decir que no veo ninguna pregunta en el formulario que tenemos para utilizar. Simplemente lo reitero. Sí tenemos una pregunta. La recibimos de Raymond Mamattah. El término farming.

JONATHAN ZUCK: La veo. ¿Farming es un término normal o lo inventé yo? Me hubiera encantado que fuera mío porque es una muy buena expresión pero en realidad es un término general bueno que tiene referencias en Internet. Una de las cosas que tenemos planificado hacer en At-Large es desarrollar la página de uso indebido del DNS en Wikipedia porque ahora no hay una sobre este tema. Esperamos desarrollarla y ver que haya una parte del ciberdelito centrada en el DNS. El uso indebido del DNS es una especie de subgrupo de lo que consideramos normalmente como ciberdelito porque se enfoca en ese tema. ¿Sí? Bien. Entonces Drew, le voy a pasar el micrófono.

DREW BAGLEY: Gracias, Jonathan. ¿Puedo compartir la pantalla para pasar las diapositivas?

YEŞIM NAZLAR: Sí, un segundo, por favor. Glenn tenía una pregunta en el chat.

JONATHAN ZUCK: La veo. No sé si la entiendo. Si hay un incremento en el phishing con COVID-19. ¿Es esa la pregunta? ¿Si hay más phishing? ¿Si hay un pico de phishing para COVID-19? Mucho. Ese es exactamente el tema que va a tratar Drew. Si para el final de la presentación de Drew todavía no tenemos una respuesta, por favor, le ruego que repita la pregunta.

DREW BAGLEY: Sé que conozco a muchos de ustedes y que me han preguntado previamente. Soy Drew Bagley, para los que no me conozcan. Estoy en la The Secure Domain Foundation, que se centra en el uso indebido del DNS. Soy el vicepresidente de Privacy and Cyber Policy en CrowdStrike, una empresa centrada en ciberseguridad. Con esas perspectivas en mente armé una presentación hoy para comentarles a todos lo que hemos observado con alguna de las últimas amenazas respecto del uso indebido del DNS en el contexto de COVID-19 y también repasar algunos de los conceptos que exploró Jonathan en su introducción con el vídeo sobre el tema para tener una idea más clara, medios para identificar y resolver el tema del uso indebido del DNS. Algunas de las tendencias que se vienen observando en los últimos dos meses en la pandemia que acecha al mundo es que los malos se están aprovechando de cualquier situación y por supuesto de esto.

Por supuesto hay un par de tendencias en este momento en que la dinámica por la cual la gente es vulnerable es un poco distinta desde el punto de vista de la ingeniería social y también desde una perspectiva técnica porque según la ubicación, la industria, las autoridades locales o requisitos en términos de cuarentena o sistemas similares, hay una serie

de situaciones diversas a nivel laboral con organizaciones que quizá pudieron implementar dispositivos corporativos para el teletrabajo u otras situaciones en las cuales las personas utilizan dispositivos personales para trabajar desde el hogar en ese entorno con menos control sobre la ciberseguridad y los datos junto con el sentido de tratar de conseguir información. La mayoría de lo que se pueda conseguir sobre COVID nos lleva a un ambiente en que se trata de diseñar ataques de phishing y de otros tipos que tratan de aprovechar a las personas que buscan información sobre COVID-19 aprovechando el hecho de que quizá las personas utilicen dispositivos personales en los cuales no tienen una seguridad en la terminal o un firewall implementado. Hay distintos ciberataques con registros de dominio que incorporan COVID-19 u Organización Mundial de la Salud u OMS o CDC, los Centros de Enfermedades de los Estados Unidos con la posibilidad de llevar gente a sus sitios o de llevarlos a los servidores de donde provienen los mails.

Les voy a mostrar una serie de ejemplos respecto a lo que estoy diciendo. Este es el directorado de ciberseguridad australiano que viene advirtiendo a la gente sobre campañas que apuntan a sitios geográficos en Australia involucrando al registro del nombre de dominio covid19-información.online. Un nuevo gTLD. Enviando SMS o mensajes de texto en lugar de mail para tratar de que la gente seleccione un link desde sus dispositivos portátiles. Ese link se utilizaría para instalar malware o software malicioso.

Hay otras cosas muy similares. Por ejemplo, en el Reino Unido con este nombre de dominio uk-covid-19-relief.com, este nombre de dominio estaba tratando de llevar a la gente a un sitio en que las víctimas ingresaban información tal como su contraseña y demás información

personal que el ciberdelincuente aprovecharía para el robo de identidad, delitos financieros y demás. Podemos ver que en ambas instancias… Volvamos un minuto a la información de WHOIS que nos muestra aquí que esos nombres de dominio están registrados muy recientemente. A menudo cuando tratan de verificar la autenticidad de un nombre de dominio hay que prestar atención a ciertas variables. Una es la fecha de registro. Aquí, por supuesto, la pandemia global es reciente también. Esa variable sola no puede ser indicativa de que sea de phishing. Si seguimos investigando, toda la información de registro está detrás de un proxy. Tenemos una dirección de WHOIS en Panamá.

Aquí los usuarios finales tratan de entender que el nombre de dominio es legítimo o no. Por supuesto, hay que seguir lo que comentaba Jonathan pero hay que utilizar WHOIS y si están ocultos los detalles eso puede ser indicativo o no de que sea algo sospechoso pero al menos hay que tener en cuenta y preguntarse si se puede confiar. Como lo vemos aquí con el registro del nombre de dominio.

No tengo el equipo maravilloso que tiene Jonathan pero para que no se me duerman vamos a tener la primera pregunta. La primera pregunta es si es fácil decir si un email es legítimo. Verdadero o falso. Cinco segundos más. Veo que están activos. Bien. La respuesta correcta es falso. No es siempre fácil saber si es legítimo porque la ingeniería social es una forma de arte. Los adversarios pueden ser muy específicos en la manera de acotar las cosas para alguien que es de una organización que espera cierta comunicación inclusive en términos de tratar de cubrir sus huellas con spoofing, conseguir la información del registro de WHOIS e inclusive la dirección de la que proviene un mail. Les muestro un ejemplo de eso.

Primero vamos a ver los resultados de la pregunta. Vemos que más de la mitad decidió que era falso, que es correcto, pero les voy a mostrar un ejemplo de un mail que es complejo. Aquí podemos ver que esto proviene de un nombre de dominio legítimo who.int y también una dirección de email asociada con la OMS, con la Organización Mundial de la Salud. Ha habido campañas además, no solamente la actual sino también hace un par de meses, donde se incorporaron eurohealthcities@who.int y dónate@who.int. El mail parece provenir de la dirección de email correcta pero no lo es. La dirección de respuesta es la que lo muestra pero hay distintas maneras de que las organizaciones puedan evitar eso agregando seguridad a los servidores para que no se los utilice para estas cosas para instalar tecnologías que permitan discernirlo pero eso es algo muy común, que se puede conseguir la información de esta manera mediante spoofing.

Quizá consiguen los encabezamientos mediante spoofing pero el cuerpo puede parecer legítimo descargando gráficas reales de otros lugares que están asociadas con la OMS. Eso es simplemente un ejemplo que nos demuestra que no siempre es sencillo ver cuál es la diferencia. Hay más ejemplos de este tipo de campañas. Me gustaría que miren el blog que está en el link que está en la parte inferior de la diapositiva. Algunas pautas para permanecer seguros.

En base a lo que decía Jonathan hace unos meses es muy importante cuando uno recibe un SMS o un mail o cualquier otro tipo de comunicación que tenga un link o que le solicite que hagan algo con dinero o con información, ese tipo de cosas, es muy importante investigar todas la sección para evitar ese tipo de cosas en primer lugar. Por supuesto, como se sugería, inspeccionar los encabezamientos pero

ese ejemplo que vimos recién quizá nos muestra que quizá no sean verdaderos. Usen WHOIS para ver si un registro de nombre de dominio parece legítimo o no. Nuevamente, quizá sea una indicación lo que pasa con el proxy que no sea legítimo. Por otro lado, también utilicen registro de proxy y los nombres de dominio legítimos pero tenemos que considerar las circunstancias y también pensar si quien nos contacte puede llamar o ponerse en contacto con alguien para verificar de dónde proviene el email o inclusive ver el ejemplo de la OMS e ir al sitio de la organización a ver si hay alguna advertencia sobre este tipo de cosas.

En los casos que les presenté, como en Australia, Reino Unido y la OMS, en los tres casos el gobierno y las instituciones tenían en sus sitios advertencias sobre estos elementos ilegítimos descubiertos. Las organizaciones advierten a la gente. Hay que tenerlo en cuenta y buscarlo y verificar que uno tenga protegidos los dispositivos con una solución de protección del terminal que sea efectiva. Eso es muy importante. Encontrar una solución de ciberseguridad que se centre, que nos permita hacer actualizaciones y parches que se hagan automáticamente, centrándose lo que puede llegar a hacer el adversario con el software malicioso para evitar también que se nos redireccione a algún otro lado.

Es importante tenerlo también en los dispositivos personales además de los de la organización. Si uno se acuerda, también en estos tiempos hay que hacer capacitación sobre el tema, elevar el nivel de concientización de la gente a nivel personas y también organización. Otra manera de probar los archivos y las URL antes de seleccionarlos es poniéndolos ante lugares de multiscanner. Por ejemplo, www.hybrid-analysis.com. Hay

varias que se pueden explorar o que pueden llegar a ser útiles. Hacer pruebas con ciberseguridad antes de implementarlo.

Ahora es el momento de la pregunta número dos. Cuál es un ejemplo de antiabuso proactivo o de antiuso ilegítimo. 15 segunditos más. Bien. Las últimas respuestas. Bien. C y D aquí serían los ejemplos. Después de haberlo utilizado para algo malo. El ejemplo que les mostré con el nombre de dominio es muy importante después de que algo se descubrió para ver que se suspenda el nombre o una cuenta completa asociada con el nombre de dominio. Investigarla si hay algún otro nombre de dominio utilizado para el ciberdelito. Hay actividades tales como las que comentaba Jonathan en el tema de uso ilegítimo del DNS donde se identifican nombres sospechosos antes de utilizarlos. Podemos buscar ciertas características que pueden estar asociadas con campañas de phishing. El registro generalizado, procesos similares si hay una cuenta de registratario asociada. También en lugar de agregar nombres de dominio. Estos son los resultados, que no están mal.

Lo que es interesante con respecto a alentar a las distintas partes interesadas a tomar una actitud proactiva son los incentivos en torno a los usuarios finales que podrían ser víctimas y también organizaciones que controlan la infraestructura porque el uso indebido del DNS no es bueno para nadie excepto para los ciberdelincuentes. Uno puede ser un registrador de un ccTLD o de un gTLD pero igualmente hay mucha presión para responder ante esas denuncias. Esto insume tiempo, tiempo es equivalente a dinero que se resta de la operación y en lo que uno puede hacer en cuanto al operatorio normal. Si encima hay incumplimiento, esto lo pone debajo del microscopio de las autoridades. Incluso la reputación en términos generales se puede ver afectada.

Posiblemente algunos no quieran hacer negocios con ustedes. Incluso un registro, puede haber TLD enteros y las empresas pueden decidir no registrar un nombre de dominio con un TLD determinado porque siempre está asociado con algún engaño, con algún problema, entonces no se lo toman en serio.

De la misma manera, cuando uno reacciona ante el uso indebido del DNS, también tiene que preocuparse por suspensión de los nombres de dominio. Tal vez un rembolso de gastos de tarjeta de crédito. Puede haber también órdenes judiciales, de juicios, pérdida de acreditación involucrados. En el contexto de la pandemia, hay nombres de dominio que se pueden identificar como spoofing de organizaciones internacionales como en el caso de la OMS o con el nombre de COVID-19, que todavía siguen siendo registrados y utilizados con éxito. Si bien hay incentivos para combatir el uso indebido del DNS, siempre es importante identificar estas cuestiones antes del hecho y someter a un rígido escrutinio a todos los sitios.

Pasemos a la siguiente pregunta, la tres. ¿A quién afecta el abuso del DNS? ¿Quién se ve afectado por el uso indebido del DNS? Muy bien. Les voy a dar unos 15 segundos más. Muy bien. Creo que tenemos un buen índice de respuestas aquí. Muy bien. Les fue fantástico en esta pregunta a todos. Eso es correcto. Incluso cuando hablamos de los incentivos financieros para las empresas, tenemos que sumarlos a todos los usuarios finales que van a ser víctimas y organizaciones que emplean a los usuarios finales que también pueden dar lugar a una amenaza importante, por ejemplo en el caso de un hospital.

Si ustedes piensan en la propagación del ransomware en los últimos tiempos y con otro tipo de ataques que hubo en las cadenas de suministros por ejemplo y de WannaCry, todos se ven afectados por la registración del DNS para fines debidos que terminan desplegando algún tipo de software malicioso y causando violaciones a la seguridad. Esto afecta a todos. Muy bien.

Pasemos a la siguiente pregunta. Quién tiene la posibilidad de prevenir el uso indebido del DNS. No sé si se está mostrando correctamente la pregunta. Tal vez necesite ayuda de quienes están administrando esto. No se está mostrando aquí la imagen de la pregunta. Ahora sí. Les voy a dar unos 15 segundos más. Muy bien. Para todos los que dijeron que todos lo hacemos, eso es correcto. La ICANN como organización y la ICANN como comunidad tienen un papel importante que desempeñar al igual que las partes contratadas. Sé que están lidiando en la primera línea con estas situaciones, que tienen que trabajar de manera proactiva investigando una registración antes de aceptarla en lugar de trabajar después del hecho, para detener las campañas de phishing o para detener este tipo de actividades. Los usuarios finales, que identifiquen e informen de las amenazas para protegerse a sí mismos. También asegurarse de tener como prioridad la ciberseguridad y luego la comunidad de expertos en ciberseguridad para explorar e investigar estas situaciones, advertir al público y también desarrollando el software pertinente de ciberseguridad para protegerlos a todos.

En última instancia, la gobernanza de Internet es un tema fundamental para combatir el uso indebido del DNS. Es por eso que, como lo dijo Jonathan, la comunidad de At-Large tiene un papel singular en la representación de los usuarios finales y en asegurarse de que en última

instancia los usuarios finales tengan voz y se pueda explicar y educar y promover soluciones que tengan un impacto sobre el uso indebido del DNS, ya sea que se trate del ALAC o de otras partes de la comunidad de la ICANN, la ICANN como comunidad puede generar incentivos para todos los actores para asegurarse de que haya un terreno común y es el entendimiento de que el uso indebido del DNS es malo para todos y que todos tienen un papel en la lucha contra este flagelo. Tomando medidas de manera proactiva, dando incentivos para que se pueda operar y trabajar para combatir el uso indebido del DNS y también para prevenir estos ejemplos tan sencillos que compartí con ustedes hoy, para que no ocurran desde el inicio, para que quien utilice spoofing para COVID-19 o quienes utilizan este tipo de estrategias en sus registraciones de nombres de dominio no puedan avanzar con ello.

La comunidad de la ICANN en su conjunto y esta unidad constitutiva en particular pueden tener un papel muy activo para luchar contra el uso indebido del DNS. También teniendo en cuenta lo que dijo Jonathan con los datos que hay ahora disponibles. Es importante para tener un abordaje bien dirigido porque hay datos que muestran cómo se están cometiendo estos ataques. Los registradores, los revendedores son utilizados para registración de determinados nombres de dominio cuya zona tiende a llevar a la registración de nombres de dominio para un uso indebido. Ahora es importante utilizar estos datos y aplicarlos en la gobernanza de Internet para prevenir el uso indebido del DNS.

Ya terminamos estas preguntas a modo de evaluación. Ahora tengo unas preguntas a modo de encuesta para ustedes. La primera es la siguiente. ¿A ustedes los han dirigido a campañas de phishing relacionadas con COVID-19? No tienen que ser necesariamente las que les mostré. A

través de SMS o de email, ¿les han llegado a ustedes campañas de phishing relacionadas con COVID-19?

JONATHAN ZUCK: En realidad hay dos preguntas en esta encuesta. Todos deberían poder bajar y verlas.

DREW BAGLEY: Sí, claro. Están las dos en la misma pantalla. La segunda es si han recibido capacitación adicional sobre seguridad cibernética de su empleador desde que comenzó la pandemia de COVID-19. La respuesta es sí o no. Les voy a dar unos segunditos más para que vayan respondiendo a estas dos preguntas.

JONATHAN ZUCK: Hola. ¿Quién está hablando?

ORADOR DESCONOCIDO: ¿Cómo podemos responder a esta pantalla? ¿Puedo decir algo ahora?

JONATHAN ZUCK: Sí.

ORADOR DESCONOCIDO: ¿Esto es algo que ustedes están compartiendo de su parte, la pantalla?

DREW BAGLEY: Sí. En realidad estamos compartiendo aquí dos preguntas de la encuesta. Acabamos de sacarlo de la pantalla y ahora vamos a mostrar los resultados. Parecería que lamentablemente algunos de ustedes, un tercio de ustedes, respondieron que sí han sido víctimas de campañas de phishing o por lo menos destinatarios de campañas de phishing relacionadas con COVID-19. Igualmente, más de la mitad de ustedes piensan que no lo han sido. Un porcentaje de ustedes han recibido capacitación adicional sobre seguridad cibernética desde que comenzó la pandemia. Por eso al principio de la presentación les decía que era muy importante tener esta capacitación ahora, porque a menudo la organización para el trabajo remoto puede ser diferente. A veces el empleado puede conectarse a través de la infraestructura de la compañía para la que trabaja mientras que en otros casos lo puede hacer por sus dispositivos personales. No es lo mismo que estar en un entorno de oficina o incluso cuando no cambie esta organización tal vez uno no esté al tanto de cómo se está utilizando la pandemia para estos fines, para tomar como objetivos a las personas, a los usuarios. Muy importante que ustedes en sus empresas ayuden a los empleados con más capacitación. Esto es lo que yo tenía para presentarles a ustedes. Con gusto voy a responder cualquier pregunta que les haya surgido. No estuve mirando el chat.

JONATHAN ZUCK: Yo le voy a hacer las preguntas para usted. Hubo varias preguntas que fueron dirigidas a usted. Una era que normalmente vemos que los registradores no responden a las solicitudes de información. ¿Usted tiene algún ejemplo respecto de registradores o registros que hayan sido de utilidad para responder a estas consultas?

DREW BAGLEY: Sí. Creo que eso pasa todo el tiempo. Ambas situaciones se dan todo el tiempo, debo decir. Los registradores y los registros, dependerá de qué registrador o de qué registro hablemos. También dependerá de las circunstancias y de cuánta atención ha recibido un nombre de dominio en particular. Ciertamente yo escuché hablar de esta situación en la que las partes no responden a estas solicitudes. No tengo un ejemplo específico para compartir o para mostrarles dónde hubo respuesta pero en mi organización sabemos que hay registradores y registros que responden y otros que no. Dependerá de cuál se trate. Algunos responden muy bien pero responden tal vez después del hecho que es muy bueno, es importante, porque esto los ayuda a buscar maneras de ser proactivos cuando aparece esta registración y para poder evitar que se perjudique a las personas. Es importante que todos sean persistentes si tienen que hacer una denuncia o un reclamo ante los registradores, los registros para que tomen conocimiento de su uso indebido y también es importante que se involucre al departamento de cumplimiento contractual de la ICANN en caso de que el registrador o registro no estén cumpliendo con su obligación de investigar y no estén dando respuesta. En términos más generales, esto que hablábamos de las recomendaciones del equipo de revisión de CCT, como mencionó Jonathan, también hay que aplicarlo para que las partes sean más proactivas.

JONATHAN ZUCK: Gracias, Drew. Otra pregunta de Samridh Kudesia, dice: “No entendí cómo la información en los encabezados puede diferir de lo que se ve en otros campos. ¿Puede explicar cómo funciona?”

DREW BAGLEY: Sí. Esto puede pasar de distintas maneras. Dependiendo de cómo estén configurados los servidores, a veces un servidor de correo saliente no está configurado con el mismo nivel de seguridad que un servidor de correo entrante. Una persona que no está vinculada con determinada organización puede poner los detalles del servidor de correo saliente para la organización a la que quiere hacer spoofing, sin necesitar ninguna credencial. Puede hacer un ping a ese servidor y obtener el email de ese servidor. Esa puede ser una manera. A veces lo que están haciendo los adversarios es no utilizar un servidor legítimo. Hacen que el encabezado parezca que proviene de un servidor legítimo registrando un nombre de dominio que es casi idéntico a la organización legítima. Pueden utilizar dos v en lugar de una w, por ejemplo. Uno utiliza esa infraestructura de correo saliente.

JONATHAN ZUCK: Gracias, Drew. Esto también se aplica a algunos IDN con las distintas escrituras ortográficas. Por ejemplo, con caracteres no latinos como en el caso de Bank of America.

DREW BAGLEY: Exactamente.

JONATHAN ZUCK: Tenemos una pregunta. Dice: “No tenemos sistemas 100% impenetrables. ¿Qué es lo que puede hacer la ICANN en este sentido, sobre todo cuando más del 70% de los ataques corresponden a algo interno de la organización?”

DREW BAGLEY: Tal vez esa organización tenga más que ver con la ICANN como organización con respecto a lo que pueden hacer cuando hay una violación de la organización de la ICANN. A diferencia de esas violaciones de datos que utilizan el DNS y que impactan otra organización y que van a involucrar un abordaje con múltiples aristas donde se vean cuáles son los servicios de respuesta en caso de que haya una infracción y también cómo se puede identificar esa infraestructura delictiva en la que están siendo alojadas estas direcciones IP para poder darla de baja. Con respecto a cómo la organización de la ICANN puede responder y responde, sobre todo cuando son ataques que tienen que ver con su organización interna, creo que lo podría responder la ICANN.

JONATHAN ZUCK: Una pregunta de Hadia Elminiawi. “¿La falta de información pública de los nombres de dominio puede dar lugar a mayores problemas en este sentido?”

DREW BAGLEY: A veces se dificulta el análisis de correlación. Incluso aunque tengamos información en WHOIS que no es verídica, si tenemos información falsa común, como una dirección de email, vamos a recibir una consulta de esa dirección de email junto con otras registraciones asociadas con esa

dirección. Puede pasar que un nombre de dominio tal vez ya se sabe que es utilizado para una conducta maliciosa, si uno hace una consulta de esa dirección va a tener 100 nombres de dominio registrados en la misma época que no han sido utilizados y también pueden tener la sospecha de que ha sido utilizado pero ahora, con el WHOIS que pasa a estar oculto, este análisis de correlación es muy difícil de llevar a cabo.

El uso de los servicios de representación y de privacidad ha sido utilizado durante mucho tiempo pero los ciberdelincuentes no siempre utilizan estos servicios de proxy. Ponen sus detalles falsos en la parte pública en lugar de hacerlo en el de proxy. Esto nos da más información para esa correlación.

JONATHAN ZUCK: Gracias, Drew. Siguiente pregunta. "¿Hay algunas aplicaciones que permitan verificar el software malicioso en el punto de ingreso que usted conozca?"

DREW BAGLEY: Uno de los basados en la web es hybrid-analysis. Yo lo mostré en mi diapositiva. Es una plataforma que hace sandboxing de ciberseguridad. Uno puede cargar un archivo y lo va a verificar y va a generar informes para que todos sepan si esto es seguro o no. Esto les muestra también una captura de pantalla con respecto a cómo se vería afectada su computadora si se ejecutara ese archivo. Hay otros también parecidos.

JONATHAN ZUCK: Gracias, Drew. "¿El uso indebido del DNS podría ser utilizado para espionaje comercial?"

DREW BAGLEY: El uso indebido del DNS puede utilizarse para todo tipo de fines. Podemos tener actores que sean estados, que utilicen el DNS para sus propios intereses. Podemos tener actores de delitos electrónicos para cometer fraude. Podemos tener hackers también que quieran alterar todo y básicamente podría ser utilizado el DNS para hacer cualquier cosa que se les ocurra.

JONATHAN ZUCK: Esto tal vez sea una acción a concretar para el personal. "¿Cuál es el tiempo de respuesta contractual de un registrador o un registro para trabajar sobre una denuncia? ¿Los datos sobre cuántas denuncias fueron recibidas y cuántas fueron resueltas están disponibles públicamente?" Se lo paso a ICANN org. Lo vamos a tomar como otro punto de acción y poner la respuesta en el wiki y en el CPWG para este webinar. Creo que esas son todas las preguntas que tenemos. Muchas gracias, Drew. Le paso la palabra a Joanna.

DREW BAGLEY: Gracias, Jonathan.

JOANNA KULESZA: Muchas gracias, Drew y Jonathan. Muy bueno para poder comentar la situación actual. La segunda es el feedback. ¿Alguien quisiera dar feedback en audio además de en el chat o algún comentario que

hayamos obviado? Veo que Gopal tiene una pregunta. “Gracias por responder mi pregunta”. Podemos hacer las preguntas con el seguimiento de Gopal. Si hay alguna cosa que hayamos pasado por alto o si hay algo que se necesite, Drew y Jonathan pueden tratar esa pregunta. No sé bien los detalles pero quizá sea más fácil que la respondan los presentadores.

JONATHAN ZUCK: Creo que podemos responder. Vamos a registrar la pregunta y verificar que esté en la lista de CPWG.

JOANNA KULESZA: También en la wiki y para este webinar. Son un paso inicial para participar en este tema y poder comprender mejor todos los temas que están relacionados con calidad. No sé si hay algún otro comentario o pregunta. Tenemos tiempo todavía. Hay una pregunta de Vivek. A ver si hay alguna acción sobre este tema.

JONATHAN ZUCK: Drew quizá quiera tomar este tema. La información que falta es el nombre de la parte contratada que está en infracción. Es difícil para los que están fuera de ICANN utilizar la ejecución propietaria. Esa es una de las cosas que defiende At-Large. Poner la información a disposición antes, tal como el nombre propiamente dicho del registratario y del registrador para poder tomar las decisiones correctas para ver si uno toma una decisión proactiva que involucra en negocios con esa parte o no.

DREW BAGLEY: Correcto. Eso es algo en lo cual si vemos el informe del CCT, una de las cosas que enfatizamos es tomar un enfoque inducido por los datos para ver qué datos utilizamos, para qué la comunidad de ciberseguridad normalmente utiliza esta información. Mecanismos para tomar acción y utilizar los datos que están allí.

JOANNA KULESZA: Muchas gracias, Jonathan. Muchas gracias, Drew. Entiendo que este es un paso adelante para dar calidad y seguridad a la información. Muchas gracias nuevamente por el tiempo para estar con nosotros. Este es un paso adelante para el proceso de desarrollo de políticas y el trabajo en ICANN. Hay un informe de feedback que quisiéramos de su parte sobre este webinar o la serie de webinars. Entiendo que Yeşim tiene una pregunta. ¿Es correcto?

YEŞIM NAZLAR: Sí, correcto. Gracias, Joanna. Si me permiten, respecto de las preguntas de la evaluación.

JOANNA KULESZA: Sí.

YEŞIM NAZLAR: Muchas gracias. Tenemos varias preguntas. Por favor, si pueden dedicarle un par de minutos a responderlas. Son muy importantes para nosotros. Se las voy a ir mostrando. La primera es cómo se enteró de este seminario web. Es un multiple choice con diversas opciones. Twitter, Facebook, la lista de correo de At-Large, el calendario, Skype,

colegas y otros. Pueden elegir todas las respuestas que quieran, por las cuales les haya llegado.

Paso a la segunda pregunta ya que pueden leer todas. ¿En qué región reside ahora? África, Asia, Australia y las islas del Pacífico, Europa, Latinoamérica y el Caribe, o Norteamérica. La tercera pregunta es qué le parece el tiempo del seminario a las 15:00 UTC. Demasiado temprano, demasiado tarde. La cuarta pregunta. La duración del seminario. ¿Da tiempo suficiente para las preguntas? Esta es una pregunta de respuesta sí o no. La quinta pregunta. ¿La presentación resultó interesante? Está de acuerdo firmemente. Estoy de acuerdo. Ni de acuerdo ni en desacuerdo. En desacuerdo. Firmemente en desacuerdo.

Pregunta siguiente. Aprendí algo de este seminario. De acuerdo firmemente. Ni de acuerdo ni en desacuerdo. En desacuerdo. Firmemente en desacuerdo. Quisiera participar en otros seminarios de At-Large. Firmemente de acuerdo. De acuerdo. Ni de acuerdo ni en desacuerdo. En desacuerdo. Firmemente en desacuerdo. La última pregunta. Voy a mantener abierta la encuesta para que puedan tomarse más tiempo para responder. Este es el final del relevamiento de evaluación. Joanna, muchas gracias.

JOANNA KULESZA: Muchas gracias, Yeşim. Gracias a todos por participar, por dar sus ideas para mejorar. Esperamos los webinars, cualquier cosa que les interese. Entiendo que no hay más preguntas ni más feedback. Iríamos cerrando. Este subgrupo del grupo de trabajo de creación de capacidades está liderado por Hadia. Muchas gracias por la presentación. Gracias por invitar a los oradores. Gracias a Jonathan y a Drew por tomarse el

tiempo de liderar este tema del uso indebido del DNS. Esto seguramente nos va a permitir participar más en el desarrollo de políticas. Este tema es crucial. Con eso esperamos que aprovechen el conocimiento o las novedades que tenemos y que puedan participar en el sitio de desarrollo de políticas y en el grupo de trabajo de consolidación de calidad.

Hay otro webinar previsto para el 1 de julio. Es un tema más general en términos de nombres de dominio y mensajes de texto, geopolítica, el proceso de desarrollo de políticas de todas las partes interesadas de ICANN en el área diplomática también. Espero poder moderar el próximo seminario. Se les van a dar novedades e informaciones. Esperamos que tengamos noticias de la junta con la perspectiva también del usuario en el webinar y también noticias de ICANN org sobre el trabajo que se viene haciendo en campo sobre el desarrollo y las relaciones diplomáticas. El 1 de junio, me dicen, acotan Claudia y Heidi. Disculpas. De todos modos se les va a informar. Con esto quisiera agradecer nuevamente a los oradores, a todos por la participación, al servicio de idiomas. Muchas gracias a todos. Cierro.

YEŞIM NAZLAR: Muchas gracias a todos por estar en el seminario. El seminario termina aquí. Muchas gracias.

[FIN DE LA TRANSCRIPCIÓN]