ICANN67 | Foro virtual de la comunidad – Sesión sobre políticas de At-Large: uso indebido del DNS: llamado a la acción de At-Large
Lunes, 9 de marzo de 2020 – 13:45 a 15:15 CUN

YEŞIM NAZLAR: Vamos a dar comienzo a la sesión en dos minutos.

MICHELLE DESMYTER: Buenos días, buenas tardes y buenas noches a todos, soy Michelle DeSmyter del personal de la ICANN. Bienvenidos a la reunión virtual de ICANN67 y a la sesión de At-Large sobre el uso indebido del DNS., es una sesión virtual de llamado a la acción el día 9 de marzo. El audio de Zoom está en inglés, para poder acceder a los audios en francés o en español deben conectarse al streaming en francés o español cuyos links se encuentran publicados en el sitio web de la ICANN, también están publicados en la dirección de correo electrónico.

También pueden pasar a la agenda de la reunión en las páginas Wiki. No vamos a pasar asistencia por cuestiones de tiempo, pero se va a tomar en cuenta la asistencia de los miembros y coordinadores de enlaces. Pueden hacer sus preguntas en inglés, en español o en francés y para eso deben agregar a sus comentarios o preguntas “question” al final y al principio o “comment” al final y al principio de cada comentario según sea pertinente.

También deben mencionar su nombre completo, el personal va a hacer un recordatorio de este proceso en el chat, también si están en la sala del chat y quieren tomar la palabra, pueden levantar la mano para que el personal los coloque en la lista de oradores. Como recordatorio, por favor mencionen sus nombres no solamente para la transcripción sino para que los intérpretes puedan identificarlos en los canales lingüísticos correspondientes.

Además, hablen a una velocidad razonable para dar lugar a una interpretación adecuada, al igual que todas las actividades de la ICANN, esta actividad también está regulada por el código de conducta de ICANN, así que voy a colocar estos principios o códigos de conducta para que ustedes los tengan a la mano. Ahora sí, le doy la palabra a Jonathan.

JONATHAN ZUCK: Gracias a todos por participar, veo que hay unos 167 participantes aproximadamente. El ALAC tomó la decisión de que el uso indebido del DNS sea uno de los tópicos más importantes para At-Large para el año 2020, así que la idea de esta sesión es tener un pantallazo general de todos los tópicos que están relacionados con el uso indebido del DNS. Esto va a ser para algunos muy básico, para algunos otros va a ser algo nuevo, pero la idea es tener un debate cara a cara de uno a uno básicamente con el tema del uso indebido del DNS porque este tema cada vez es un tema más importante.

En este caso hay un llamado a la acción y un plan que At-Large diseñó como campaña para implementar a lo largo del año. En la agenda ustedes verán que hay enlaces a un video y a esta presentación en inglés, en español y en francés, así que, si ustedes tienen problemas en la conexión de Zoom, estos videos también van a estar disponibles en YouTube y los pueden ver a través de estos links en lugar de verlos a través de Zoom.

En caso de que tengan problemas con la banda ancha o que deseen verlos posteriormente, están disponibles en los tres idiomas y los enlaces como dije anteriormente, están colocados en la agenda. Así que lo que vamos a hacer es que vamos a pasar la versión en inglés y vamos a contar con la interpretación en francés y español de estos videos, pero por favor utilicen los links en la agenda si así lo desean, para escuchar los videos en los idiomas pertinentes si es que les resulta más fácil.

Así que, sin más, vamos a colocar el video. Adelante, por favor.

JONATHAN ZUCK VIDEO: Buenos días, buenas tardes, buenas noches y para quienes son menos afortunados, buena madrugada. El desarrollo de políticas de la ICANN es engañosamente complejo, dada la misión relativamente simple de las organizaciones, es fácil pasar por alto las cuestiones más importantes cuando estamos ocupados en cuestiones menores.

Como los únicos representantes de los usuarios finales y sus intereses es crítico que no perdamos el foco, en lugar de ello debemos identificar

las grandes cuestiones que enfrentan los usuarios individuales y ser defensores acérrimos para mejorar esas áreas.

Quizás la amenaza más compleja a estos usuarios es el uso indebido del DNS. Hoy vamos a hablar del uso indebido del DNS para que sea parte de todas las conversaciones que tenemos en la comunidad de la ICANN. Entonces en lugar de la vieja expresión: "¿Qué has hecho por mí últimamente?" la expresión de At-Large será: "¿Qué está haciendo usted por el uso indebido del DNS?"

¿Qué es el uso indebido del DNS? Este es un término que hace tiempo está dando vueltas y que ha dado lugar a mucho debate dentro de la ICANN. En realidad, luego de la revisión de la competencia, elección y confianza de los consumidores, la Junta Directiva inició otro esfuerzo para definir el término para que pueda diseñar un mejor plan de ataque. Irónicamente aun cuando se utiliza la definición más conservadora en la cual todos están de acuerdo, se puede diseñar un marco para combatir el uso indebido del DNS y simplemente utilizarlo con más frecuencia conforme se expanda esa definición.

Todos estamos familiarizados con el DNS, Sistemas de Nombres de Dominios, es un sistema relativamente sofisticado de preguntas y respuestas que nos llevan a cualquier parte en la red mundial, es como la búsqueda del tesoro en la cual uno le pregunta a alguien el nombre de la persona que conoce, el número de la persona que uno quiere contactar.

Por supuesto, como se dice en las películas, tanta pregunta hace que los malos se den cuenta, es como pedirle a Dorothy que le pregunte al mago de oz.

En otras palabras, el uso indebido del DNS son ataques o una acción delictiva del mismo, algunas personas analizan esta definición y hablan de una definición más compleja de ataques sobre el uso indebido del DNS o ataques mediante la utilización del mismo, pero nosotros nos vamos a referir a esto como uso indebido del DNS. Uno de los ataques más conocidos es el ataque de denegación de servicio distribuido o DDoS.

Aquí se utiliza una red de computadoras zombis para efectuar tantas consultas que los servidores se saturan, a veces el elemento delictivo se interpone entre nosotros y el servidor impide información, esto se puede hacer con un ataque intermediario o con el envenenamiento del caché del DNS.

Básicamente las consultas se interceptan y se obtiene un número equivocado del sitio al que se desea acceder, estos re direccionamientos del lado del servidor se utilizan para lo que se llama un ataque de farming, es decir, un phishing sin un señuelo. Uno es redirigido a un sitio con una apariencia similar a la que desea acceder, pero cuyo fin es capturar sus credenciales de acceso.

Uno cree que accede a su banco, pero lo que hace es completar un formulario para que los hackers lo utilicen en el sitio web del banco real.

Uno de los usos indebidos más conocidos es el phishing, una manera menos técnica de dirigirlo a un servidos equivocado es simplemente pidiendo que uno lo haga, en este caso se recibe un correo electrónico donde se le pide que se loguee a su cuenta bancaria y cuando hace clic en el link uno es llevado a un sitio. Este proceso se llama phishing, uno es engañado con un señuelo y dirigido a un sitio fraudulento.

Por ejemplo, aquí vemos lo que podría leer un correo electrónico, representan algún tipo de situación compleja que requiere una solución inmediata para que uno no tenga mucho tiempo para pensar e ingrese a la cuenta.

Por supuesto, llevarlo a un sitio fraudulento no es el único objetivo que tienen estos correos electrónicos, a veces simplemente tienen adjuntos malware.

Un área de particular interés en At-Large son los IDNs o los Nombres de Dominios Internacionalizados que utilizan caracteres no latinos, estos dominios relativamente nuevos son esenciales para conectar a los próximos 4.000.000 de usuarios en internet. Y en el 2012 pudimos registrar nombres de dominios en idiomas, como, por ejemplo, ruso, árabe y chino.

Por supuesto, con cada nueva innovación los delincuentes también innovan y los IDNs no son la excepción. Resulta que hay muchas letras en el alfabeto no latino que son muy similares a las del alfabeto latino, ¿quién imaginaría que existen tantas maneras de deletrear Bank of América? Cuando uno lee esto rápidamente, ¿por qué no haría clic?

Además de recabar las credenciales, estos correos electrónicos falsos y sitios webs tienen un objetivo primario que es plantar software en sus computadoras. Esto generalmente se denomina malware, pero hay muchas variedades de malware.

Habrán escuchado de este tipo de programas que muchos de ustedes o cuyos miembros de la familia quizás hayan sido víctimas, no vamos a entrar en detalles, pero independientemente de que sea spyware o ransomware definitivamente uno no los quiere en sus computadoras. Desafortunadamente las infecciones por malware están en aumento, en los últimos 10 años se ha llegado a un 700%, como ejemplo, los ataques de ransomware se han incrementado en 350% solamente en el 2018.

Especialmente después de la revisión de la ronda del 2012 de TLDs en relación a la competencia, elección y confianza de los consumidores, los colegas de cumplimiento contractual de la ICANN hacen su mejor esfuerzo, el equipo de cumplimiento contractual comenzó a publicar datos más granulares y comenzó con su proceso de auditoría de una manera menos aleatoria, pero todavía esto no es suficiente.

Habrán escuchado hablar del informe de actividades de uso indebido de dominios que la ICANN comenzó hace unos años, aunque los informes mensuales brindan información actualizada, no brindan información suficiente para abordar el problema. Sin embargo, al utilizar DAAR podemos determinar que el porcentaje del uso indebido bajo al 1% desde su creación hace dos años.

Así que todos estaremos de acuerdo que el uso indebido del DNS es un problema para los usuarios finales. Ahora, ¿qué puede hacer At-Large en este sentido?

At-Large tiene un enfoque doble para combatir el uso indebido del DNS, la difusión externa – outreach y el proceso de desarrollo de políticas de la ICANN. At-Large va a desarrollar materiales educativos para que los usuarios finales se puedan proteger contra el uso indebido del DNS. At-Large es único en su estructura y hace posible distribuir la información a las organizaciones regionales de At-Large o RALOs que a su vez pueden distribuir esos materiales a las estructuras de At-Large.

Cada una de las cuales cuentan con individuos que pueden también distribuir estos materiales, At-Large ha desarrollado esta red durante años y que mejor otro uso podría tener que proteger a los usuarios finales de los delincuentes de internet.

Es necesario ayudar a los usuarios finales a que se protejan de las trampas. Parece una ironía constante que los delincuentes obtengan la información, no porque sean ingenieros informáticos inteligentes sino al igual que sucede en las películas, porque son ingenieros sociales muy inteligentes, en breve cuando quieren una contraseña simplemente la piden, esto fue así antes de internet y sigue siendo así el día de hoy.

At-Large tiene que educar a sus usuarios para que estén al tanto de cosas que parecen muy buenas o muy malas, siempre hay maneras de darse cuenta de si un correo electrónico es falso. Nos gusta burlarnos de esos correos de phishing porque tienen una gramática muy mala,

pero lo que no nos damos cuenta es que esa redacción es intencional porque desencadena la eliminación por parte de algunos usuarios o la compasión por aquellos que son menos sofisticados y At-Large ciertamente puede ayudar a los usuarios finales a discernir en la autenticidad de un correo electrónico no esperado.

No hace falta decir, pero en At-Large lo vamos a decir de todas formas, que los usuarios individuales deben tener protección antivirus en sus PCs y dispositivos móviles.

En realidad, en los Estados Unidos donde uno esperaría una sofisticación considerable por parte de los usuarios, el 50% de las computadoras no cuentan con protección antivirus. At-Large debe alentar a los usuarios finales que pidan a sus empleadores que implementen o que tengan servidores con las DNSSEC habilitadas para evitar los ataques de intermediarios.

Otro lugar en el cual At-Large debe hacer escuchar su voz es en los corredores, reuniones y conferencias que componen el proceso de desarrollo de políticas de ICANN, At-Large participa en este desarrollo de políticas en todos los puntos y puede ser en alguna ocasión, en una conversación en un pasillo o en un grupo de trabajo, participaremos activamente en las defensas de las mejoras dentro de la ICANN y también en las organizaciones que sirven a los usuarios finales, como por ejemplo, los registros y registradores.

En otras palabras, si alguien nos pregunta sobre el clima lo que vamos a hacer es extender la mano, mirar al cielo y decir: “Bueno, parece que hoy se va a hablar sobre el uso indebido del DNS”.

Afortunadamente no estamos solos, la mayor parte de la comunidad de la ICANN está preocupada por el uso indebido del DNS y duda de dar lugar a una siguiente ronda, una minoría no puede lograr que esta ronda se aplique sin la aceptación del resto de la comunidad de la ICANN y At-Large continuará junto con otros grupos de la comunidad llamando la atención al respecto.

Nuestra primera tarea es hacer una alto, no debería haber una nueva ronda hasta que no se aborde el uso indebido del DNS de una manera significativa, el cumplimiento contractual necesita una visión holística, no pueden simplemente reaccionar a todos los reclamos sin facultades auditoras para poder reconocer estas cuestiones.

Necesitamos también limitar las registraciones masivas porque esto tiene una alta relación con el uso indebido del DNS, por supuesto, hay usos legítimos para este tipo de registraciones y esto va a incrementar con el internet de las cosas, pero At-Large tiene que seguir defendiendo esta actividad, quizás al requerir autenticación a un registratario masivo legítimo.

El equipo de revisión del CCT y también el equipo de revisión de estabilidad y seguridad han diseñado y sugerido a la ICANN que diseñe incentivos para adoptar mejores prácticas, ciertamente se puede investigar más y esto fue recomendado por el CCTRT, el SSRT y el ALAC

y ahora por VeriSign. Básicamente hay 20.000.000 más en el presupuesto para invertir en materia de seguridad y estabilidad del DNS.

Y ciertamente están esos registros y registradores que invierten significativa cantidad de tiempo y dinero en combatir el uso indebido, en realidad hay 48 compañías que han firmado compromisos de mejores prácticas, es muy bueno, pero todavía tenemos que seguir mejorando, incluso los buenos actores pueden desempeñare mejor, así que At-Large tiene que estar atento a esto.

Es como el viejo dibujo animado de Dilbert en el cual se les recuerda a todos que una vez que se adoptan las mejores prácticas, estas mejores prácticas ya se tornan normales y ya dejan de ser las mejores prácticas, los delincuentes no son la excepción.

Entonces incluso aquellos que son buenos actores pueden desempeñarse de la mejor manera. Lo que se puede decir es que esto es una crisis de la cual nadie escapa, hay mucha investigación en cuanto a machine learning para detectar el uso indebido en tiempo real y poder predecir si una registración va a tener un fin ilícito.

Las pruebas iniciales muestran que un 80% de exactitud necesitamos para garantizar que continúe esta investigación y que se implementen sistemas para protegernos de la próxima generación de ataques y esto se puede hacer solo en una Unidad Constitutiva que son los usuarios finales. Y es en post del interés de estos usuarios finales que At-Large está trabajando.

El uso indebido del DNS nos afecta a todos, entonces lo tenemos que tener muy claro, no tiene sentido hacer un uso indebido del DNS, para más información pueden dirigirse a atlarge.wiki/dnsabuse. Muchas gracias.

JONATHAN ZUCK: Bueno, gente muchas gracias por seguir esta presentación. Si les parece les mostramos la página sobre el uso indebido del DNS para que vean que hay, pero no es más que el comienzo, vamos a tener un lugar central para el trabajo que estamos haciendo sobre el uso indebido del DNS. Está en recursos, ahí están los tres videos, si quieren volver y revisar lo que acaban de ver en inglés, están también en español y en francés.

Ahí están los vínculos de las versiones de estos videos y bueno, ahora entonces abrimos a preguntas. Alan Greenberg, adelante.

ALAN GREENBERG: Excelente ejemplo del tipo de cosas que nos gustaría que la ICANN produzca, es un placer para mí ver que nosotros estamos liderando el camino aquí.

JONATHAN ZUCK: Gracias, Alan. Volker, adelante.

VOLKER GREIMANN: Gracias, Jonathan. Sí, creo que es un buen esfuerzo para ir en contra del uso indebido del DNS, podrían haber mencionado también que los

registradores y los registros tienen o han sido muy elocuentes en la publicación del marco en la lucha contra el uso indebido del DNS que está en dnsabuseframework.org, que detalla básicamente cómo los registros y los registradores ya manejan el uso indebido.

Gran parte de los casos de uso indebido están detallados, ya han sido resueltos y se manejan regularmente, así que muchas gracias por esta presentación que detalla un problema que muchos de nosotros ya tenemos que manejar cotidianamente. Muchas gracias.

JONATHAN ZUCK: Gracias, Volker. Y muchas gracias al grupo de registros y registradores que se incorporaron a estas mejores prácticas y ya las aplican. Los signatarios son de los dos grupos, no mencioné este sitio del marco dnsabuseframework.org, sugiero que lo visitemos.

Entonces hay registros y registradores, hay algunos que hacen más que otros en la lucha contra el uso indebido del DNS y quiero en ese sentido resaltar este punto, el problema es que los malos actores existen, cómo manejar esos TLDs o registradores que todos sabemos que existen.

La cuestión es cómo manejar los malos actores de una manera tal que no signifique una carga o un obstáculo para los buenos actores, es un tema de discusión, pero es un tema, sigue siendo un problema a pesar de los mejores esfuerzos de los 48, así los llamamos y nos gustaría ver o conocer mejores prácticas de parte de ustedes, así la ICANN puede manejar mejor los malos actores. Natalie, adelante.

NATALIE: Muchas gracias por componer este video, muy informativo. ¿Podría incorporarse alguna recomendación acerca de cómo manejar el uso indebido del DNS en ICANN Learn como si fuera un módulo?

JONATHAN ZUCK: Gracias, Natalie. Qué buena idea y es algo que vamos a considerar hacer definitivamente, estamos tratando de ver todavía cuál sería el mejor plan de difusión externa, a lo mejor como parte de ICANN Learn o a lo mejor como un sitio dedicado para los usuarios finales.

La idea detrás de todo esto es que la educación puede jugar un gran papel a la hora de mitigar el tema porque tiene mucho que ver con que la gente sea engañada y dan sus contraseñas o abren un adjunto y eso es algo que tenemos que trabajar y, ICANN Learn podría ser parte de este esfuerzo.

Ahora le voy a dar la palabra a Joanna en un instante, quien en este momento está trabajando en un curso de ICANN Learn sobre el proceso de desarrollo de políticas y a lo mejor ella nos puede explicar un poquito más cómo poner en contexto respecto del uso indebido del DNS.

JOANNA KULESZA: Me complace primero ver tanta participación y con respecto a los comentarios, resalto que deben ser breves. Estas sesiones también son

sesiones de difusión externa, así que aquellos que tengan alguna pregunta no duden en formularla.

Brevemente estamos trabajando en un curso de ICANN Learn sobre los fundamentos del proceso de desarrollo de políticas de At-Large etc., y el uso indebido del DNS es uno de los temas prioritarios de la agenda, entonces una de las vías que consideramos es cómo hacer un curso de ICANN Learn que enseñe a manejar el uso indebido del DNS. Queremos asegurarnos de que el texto que incorporemos sea comprensible fuera de la ICANN.

DNS ya de por sí es un acrónimo, entonces vamos a prestar mucha atención para que esto sea claro, comprensible y fácil de entender en la comunidad de análisis de la ciberdelincuencia.

Esta presentación fue un excelente intento, muy atractivo y que puede incorporarse en una plataforma de ICANN Learn y también en otros recursos que nos gustaría poner a disposición de toda la comunidad, trabajando estrechamente con las RALOs para poder encarar las necesidades y las expectativas locales del mejor modo.

Ese es el plan general con respecto a la creación de capacidades, proporcionar recursos y este plan incluye un curso en ICANN Learn, pero como ya dije, estoy abierta a recibir las opiniones en el grupo de trabajo de creación de capacidades, contáctenos a Alfredo o a mí, o simplemente participen en nuestras llamadas. Muchísimas gracias.

JONATHAN ZUCK: Gracias, Joanna. Sí, así es, recibimos con beneplácito todo tipo de sugerencias y es un mensaje éste, este puede ser un módulo de un curso en desarrollo o ser parte de algo más amplio para un público dedicado, todavía estamos discutiendo esto internamente. Natalie, asumo que su mano es de su intervención anterior.

NATALIE: Perdón, olvidé retirarla.

JONATHAN ZUCK: No hay problema. Russ, adelante.

RUSS MUNDY: Gracias, Jonathan. Es un placer ver que se incluyó esta presentación porque es un aspecto, la educación que mitigaría las capacidades de la gente que quiere hacer uso indebido del DNS. Noté que el texto o las palabras se relacionaban cuando se mencionó DNSSEC, se hablaba de que la gente les pida a sus empleadores que tengan sitios seguros con DNSSEC y está bien – eso es lo que las empresas debieran hacer.

Pero creo que igualmente importante en especial desde la perspectiva del ALAC, sería muy apropiado también pedir a los individuos, a las personas que les pidan a sus proveedores de servicios de internet también capacidad para DNSSEC o que los mismos proveedores, los ISPs tengan zonas firmadas con DNSSEC. Eso dificultaría mucho más los ataques o el uso indebido del DNS.

Quizás sueno demasiado defensor del DNSSEC y lo soy, pero es un área que nos importa. Y para concluir debo decir que es una de las mejores presentaciones que he visto sobre el uso indebido del DNS. Gracias.

JONATHAN ZUCK: Bueno, buen punto. Estaba pensando qué podía pedirles o qué podíamos pedirles a los usuarios finales que hagan, entonces está muy bien quizás sus sitios web necesiten DNSSEC, buena sugerencia. A medida que desarrollamos los recursos para educación de los usuarios vamos a tomar nota de esto y vamos a incorporarlo para las acciones de los usuarios finales, así que gracias Russ por plantearlo.

Ephraim, adelante.

EPHRAIM KENYANITO: Hola, disculpas. Quería saber con respecto al aprendizaje de máquina automático, quería saber sobre un punto que se mencionó antes; el tema de investigación.

JONATHAN ZUCK: ¿Podría repetir su comentario?

EPHRAIM KENYANITO: La detección automática de actividades maliciosas.

JONATHAN ZUCK: Sí, los sitios fueron: .EU que está liderando el esfuerzo que ha hecho mucha investigación y también creo que fue .UK que está comenzando a experimentar. Hay un White paper muy bueno sobre .EU y los experimentos que dan muchos detalles sobre las metodologías y los éxitos que están logrando con herramientas analíticas predictivas, así que les sugiero que lo busque y si no yo me voy a ocupar de incorporarlo a la agenda para que lo encuentre.

Pero hay una publicación muy buena que hizo .EU sobre herramientas analíticas predictivas y lo que están haciendo. Esperamos ver más cosas y que esto se convierta en una mejor práctica, además de las que vemos con las que están haciendo los buenos actores en el marco de prevención del uso indebido del DNS.

EPHRAIM KENYANITO: Son los únicos dos registros que usted conoce, me pregunto, ¿si hay alguno en Asia también? O en otras partes del mundo que estén ocupándose de esto.

JONATHAN ZUCK: Por lo que sé son los únicos dos, pero no tengo la certeza. Creo que hay investigaciones en curso en .EU sí y también hay una investigación muy interesante desde Asia sobre aprendizaje de máquina que está por salir, si me manda un email le voy a contar más.

Se mencionó en un comentario reciente enviado a la organización de la ICANN el día de San Valentín, o sea que se hizo el 14 de febrero, hicimos

referencia a esta investigación que es sobre la identificación en tiempo real de instancias de ocurrencia de uso indebido del DNS, hay mecanismos predictivos, hay muy buena investigación que se está haciendo en Asia en la detección del uso indebido del DNS en tiempo real, eso viene de Asia.

Esos son los dos que yo conozco.

EPHRAIM KENYANITO: Muchas gracias.

JONATHAN ZUCK: Adelante, Laureen.

LAUREEN KAPIN: Hablo en carácter de abogada que trabajo en la Comisión Federal de Comercio de Estados Unidos, el sitio de ftc.gov que habla sobre la defensa del consumidor tiene mucho materiales interesantes, algunos que hablan específicamente de cómo identificar y evitar los ataques de suplantación de identidad o phishing están también disponibles en español e inglés y además si es una organización la que quiere utilizar estos materiales e incorporarle el logo esto también o podemos facilitar.

Así que quiero entonces invitar a la gente a que consulten estos materiales educativos porque han sido redactados por expertos en la creación de mensajes amigables para el usuario que son fáciles de

comprender, incluso si su idioma no es inglés o español, son materiales muy eficaces y si alguien tiene preguntas no duden en contactarme en privado.

JONATHAN ZUCK: Gracias, Laureen. Si le parece ponga en el chat la URL de estos materiales, seguramente la gente los encontrará muy interesantes y no dude que vamos a aprovechar su oferta de poner el logo en estos recursos. Una de las ventajas que tiene At-Large respecto de otras Unidades Constitutivas es que tenemos una gama de organizaciones participantes muy amplia.

Tenemos cincos RALOS, Norte América, América Latina y Centro América, Asia, África y Europa y dentro de estas cinco grandes organizaciones hay cientos de las que se llaman estructuras At-Large que suelen ser pequeñas entidades sin fines de lucro o personas físicas que también son miembros de las RALOs.

Entonces nuestra intención es utilizar esta estructura, este árbol para contactar o llegar a los usuarios finales y hacerles llegar estos materiales, entonces cuando hay buenos materiales para la gente solo los reenviamos, generamos los propios y usamos esta red para hacerlos llegar al público. Marita Moll.

MARITA MOLL: Gracias. Fantástico el video y llegará a gente que tiene un conocimiento muy general, hay distintos niveles de conocimientos y para aquellas

personas que quieren saber más sobre en qué no clicar esto es muy bueno. Tenemos que asegurarnos en primer lugar, que los mensajes no lleguen y para ello hacer la mayor cantidad de procesos para que los mensajes no lleguen a los buzones de entrada de la gente. Muchas gracias por este esfuerzo.

JONATHAN ZUCK: Sin duda Marita. Este video en realidad no es el que vamos a usar para la educación del usuario final para eso vamos a elaborar otros materiales, este video apunta a los participantes actuales o potenciales de At-Large para que se involucren en esta campaña, para que se entusiasmen y alcen la bandera de lucha contra el uso indebido del DNS porque será un tema muy importante para At-Large este año que entra.

Ephraim, ¿usted tiene otra pregunta? ¿O es la mano de su intervención anterior?

EPHRAIM KENYANITO: Perdón, es una mano anterior, pido disculpas.

JONATHAN ZUCK: No hay problema. Mason, adelante.

MASON COLE: Muchas gracias, Jonathan. Primero, un aplauso para el video, muy bien hecho. Quería mencionarle al ALAC que la Unidad Constitutiva de negocios BC ha trabajado mucho en uso indebido del DNS desde hace

cinco o seis meses, publicaos una declaración en Montreal, está en el sitio web en la página, lo puedo poner en el chat el vínculo y también hubo un intercambio entre BC y la Junta Directiva de la ICANN recientemente sobre el tema de qué puede hacerse en cooperación con las partes contratadas para el tema del uso indebido del DNS.

Entonces solicitamos el apoyo de At-Large, si están dispuestos a ser más activistas, más militantes ante la organización de la ICANN, para ser más proactivos con respecto al uso indebido del DNS.

JONATHAN ZUCK: Fantástico, gracias. Y nos gustaría trabajar con ustedes, hemos visto los comentarios y sabemos que ustedes tienen miembros individuales que están muy comprometidos en la protección de los clientes, así que creo que hay muchas series de cooperación entre At-Large y la Unidad Constitutiva de negocios sobre este tema, así que esperemos hacerlo.

MICHELLE DESMYTER: Tenemos un comentario Jonathan.

JONATHAN ZUCK: Perfecto.

MICHELLE DESMYTER: ICANN tiene formularios que no son fáciles de chequear, una buena idea sería pedirle a ICANN que permita reportar desde el sitio web el uso indebido. Y también hay un sitio sobre spam, phishing, etcétera.

JONATHAN ZUCK: Bueno, gracias. No veo el enlace en el chat, pero lo voy a buscar. Analicemos esas posibilidades también, el WHOIS es algo que está adoptando otra forma como resultado del GDPR y los esfuerzos del EPDP, pero si nos focalizamos desde el punto de vista de políticas es necesario garantizar o ver cuánto se puede automatizar el proceso de, por ejemplo, las agencias de protección de los consumidores, que tengan un acceso que sea menos complejo y ver qué datos se pueden tener en cuenta para seguir brindando un servicio y combatir el uso indebido del DNS.

MICHELLE DESMYTER: Jonathan, si me permite tenemos otra pregunta.

JONATHAN ZUCK: Adelante.

MICHELLE DESMYTER: La pregunta es de Ram Mohan: "¿Estos temas de higiene se tienen que tener en cuenta? Por ejemplo, no tocarse la cara, lavarse las manos, no abrir un correo electrónico, etcétera, etcétera…"

JONATHAN ZUCK: Bueno, en algunos de alguna forma en realidad es así, primeramente es un tema de higiene si se quiere, hay ciertos tipos de infraestructuras que hacen un uso indebido del DNS que no son cuestiones de higiene si

se quiere o no tienen que ver con el control que el usuario final pueda hacer sobre la higiene del DNS, sino que tiene que ver con el DNSSEC, por ejemplo, los ataques intermediarios y los usuarios finales no tienen la capacidad de poder evitar esto, pero sí un usuario final podría evitar este tipo de usos indebidos a través de la educación.

Entonces habiendo dicho esto, hay mucho que podemos hacer, por ejemplo, incrementar la fricción con las registraciones masivas y también algunas otras cuestiones en cuanto a los datos analíticos y ver de qué manera podemos ayudar a los usuarios finales para que todos creemos el hábito de no hacer clic siempre en todas las cosas que nos llegan.

Entonces si uno, por ejemplo, lee un correo que dice: “Banco de América”. Pero una letra no es o parece ser distinta bueno, eso es algo difícil de decidir incluso si se trata de un usuario final muy sofisticado, así que me parece que tenemos que hacer una combinación de esfuerzos entre quienes estamos dentro de la comunidad del DNS y los usuarios que pueden educar para poder ver una diferencia en cuanto a lo que es el uso indebido del DNS.

¿Hay alguna otra pregunta? Bueno, estaba viendo o tratando de encontrar alguna manera interesante de que la reunión virtual se hiciera diferente, que fuera un poco más interesante, así que la siguiente parte de la agenda es un quiz porque queremos que nos ayuden a reforzar los tópicos que estamos abordando y de los que aprendemos, así que si ustedes quieren participar pueden hacerlo en sus computadoras o en sus dispositivos móviles, tienen que ir a

atlarge.wiki/daquiz allí se van a poder registrar para poder acceder, utilizar el buscador y esto les va a permitir usar el teléfono como controlador o la PC o la Tablet.

Así que lo que pueden hacer es ir a: atlarge.wiki/daquiz, alguien veo que lo ha colocado en el chat, muy bien así que con eso podemos dar inicio al quiz, les doy un minuto para que se alisten y luego les doy otro minuto para que estén listos para responder preguntas, así que vamos a esperar unos minutos.

Perdón, pero no tenía mi micrófono habilitado. ¿Pueden todos ver la pantalla?

MICHELLE DESMYTER: Sí, la vemos.

JONATHAN ZUCK: Bueno, entonces vamos a darles unos segundos más para que ingresen. Básicamente van a ver allí una pregunta con opciones múltiples y les vamos a dar 20 segundos para responder la pregunta, si son unos de los primeros en responder correctamente van a tener créditos extras y luego vamos a mostrar las respuestas antes de que surja la siguiente pregunta. Así que creo que ya hay gente que está lista y perdón, pero tenía mi micrófono deshabilitado así que si estamos listos vamos a comenzar.

No sé si necesitan que lo lea, ¿serviría que lo lea yo o no? Estoy tratando de ver si puedo poner algo de música de fondo. Que es un

intermediario, una canción de ABBA de 1975, un tipo de ataque de uso indebido del DNS alguien que puede darle poder en el videojuego [Dauntless]. Que es una herramienta importante para combatir el uso indebido del DNS, la educación, el DNSSEC, la encriptación, lavarse las manos.

SÉBASTIEN BACHOLLET: Jonathan somos 220 y pico de personas en línea y hay sólo unos 50 participantes, no sé qué están haciendo, pero me parece que no es un buen uso del tiempo.

JONATHAN ZUCK: Gracias, Sébastien, no es nada más que un experimento.

SÉBASTIEN BACHOLLET: Sí, pero un experimento con 230 personas tiene que estar mejor diseñado.

JONATHAN ZUCK: La siguiente pregunta es, "¿qué son homógrafos?"

ALAN GREENBERG: Los que están respondiendo quizás no están respondiendo bien a propósito.

VOLKER GREIMANN: ¿Cómo se llama un email que le lleva a un sitio web falso? ¿Un email de lápiz envenenado, un email de phishing o un email de spam? ¿Cómo se llama todo el software malo que se incorporó a la computadora? ¿Virus? ¿Malware o software malicioso? ¿O intermediario?

¿Cuánto ha crecido la infección de malware en 10 años?

ALAN GREENBERG: Hay un error de tipeo en la palabra en inglés malware.

VOLKER GREIMANN: Me parece que no fue un error de tipeo sino intencional con la palabra “male” que en inglés es masculino.

ALAN GREENBERG: Creo que aquí la primera es la respuesta correcta. ¿Cómo puede la inteligencia artificial ayudar con el uso indebido del DNS? La primera es, nos hace más inteligentes, los robots buscan en internet sitios webs malos, nos ayuda a predecir la intención para hacer cosas malas.

VOLKER GREIMANN: ¿Cuál de estos botones entonces es malware o software malicioso?

JONATHAN ZUCK: Cállese la boca. Siguiente pregunta, ¿cuál es la manera más sencilla de conseguir la contraseña de otra persona? Un ataque de intermediario.

ALAN GREENBERG: Es intermediario, alguien en nuestra contra.

ROD RASMUSSEN: Usted tiene razón, Alan.

VOLKER GREIMANN: Es sorprendente, pero en muchos casos es así.

JONATHAN ZUCK: Muy bien, parece que tenemos aquí a los ganadores, muchas gracias a todos por participar en este experimento, era para hacer un poquito más interactiva esta primera reunión virtual de la ICANN un poco más interesante. Algo más que quisiera hacer para cerrar, es contarles un poquito sobre las otras sesiones sobre el uso indebido del DNS que sucederán próximamente, hay una sesión sobre herramientas holísticas para cumplimiento contractual.

Es una sesión con Jamie Hedlund de cumplimiento contractual de la ICANN y James Bladel que es el director de política de GoDaddy, que vamos a analizar una serie de escenarios y cuál sería la mejor manera para que cumplimiento contractual pueda manejar esos escenarios, recibiremos las opiniones de ambos.

Y lo que esperamos que surja de estas conversaciones es una determinación de si cumplimiento tiene las herramientas para luchar proactivamente contra el uso indebido sistémico y no lo que está

ocurriendo que es reactivo. Entonces sobre eso hablaremos en la próxima sesión y luego tenemos otra sesión que me gustaría o le voy a pedir a Joanna que nos cuente, qué viene después. Joanna cuéntanos acerca de tu sesión y de qué se hablará.

JOANNA KULESZA: Muchas gracias. En esa nueva sesión hablaremos de temas de ciberdelincuencia y ciberseguridad, hay un vínculo sobre el tema, es una buena oportunidad para mí para trabajar con Jonathan quien sabe mucho del tema, intentaremos explorar en esta sesión el tema de la soberanía del software y el ámbito de la ICANN en este tema.

Estará Veni Markovski quien ha publicado un informe sobre ciberseguridad y ciberdelito, León ha aceptado gentilmente también participar, Patrik Falstrom nos dará algunos antecedentes del aspecto técnico, también tendremos participación de la NCUC sobre la cibersoberanía y luego Jonathan nos hablará sobre el informe pragmático del cumplimiento en la lucha contra el uso indebido del DNS.

Analizaremos el aspecto geopolítico, los temas que estarán en la agenda de la Junta Directiva en los próximos años, intentaremos trazar vínculos entre las cosas que están pasando por fuera de la burbuja de la ICANN desde la perspectiva de los usuarios individuales y su ciberseguridad.

Como mencioné en el chat, también nos gustaría explorar el tema del uso indebido del DNS y su relación con otros intereses de los usuarios

individuales, es decir, qué es lo que los usuarios individuales esperan, cómo esperan estar seguros en línea para ver dónde están las relaciones que ellos tienen con el ciberdelito, la ciberseguridad, los derechos individuales, la privacidad, la libertad de expresión, la protección de la propiedad intelectual, etcétera, etcétera.

En esta sesión queremos ver el gran panorama, por eso tiene un signo de interrogación el título de la sesión “un mundo, una internet” es una interrogante. Muchas gracias por estos minutos, Jonathan y por esta gran introducción del uso indebido del DNS, esperamos contribuir al debate dentro de la ICANN, pero también por fuera de la ICANN en este tema de la ciberseguridad. Muchas gracias.

JONATHAN ZUCK: Gracias, Joanna. Muy entusiasmado por su sesión, será una gran sesión intercomunitaria así se planeaba en Cancún, esperamos tener muchos participantes así que tratemos de participar. Y hoy, más tarde tendremos una sesión sobre herramientas holísticas para el cumplimiento.

Bien, esto es todo de mi parte a menos que el personal me indique que queda alguna pregunta.

MICHELLE DESMYTER: Un momento Jonathan, quisiera confirmar. No hay más preguntas.

JONATHAN ZUCK: Fantástico, muchas gracias a todos por participar. Gracias Volker por darnos esta información sobre el sitio nuevo y el marco dnsabuseframework.org, también al final del video habrán visto que hay un sitio web para saber dónde está trabajando At-Large sobre este tema que es atlarge.wiki/dnsabuse, así que visítenlo y sigan nuestro trabajo, es esa página del sitio web de At-Large. Muchas gracias por participar, la pasamos muy bien gracias.

MICHELLE DESMYTER: Muchas gracias, Jonathan y gracias a todos. Se cierra la sesión.

[FIN DE LA TRANSCRIPCIÓN]