ICANN84 | Reunión General Anual – Reunión conjunta: el GAC y la ccNSO
Miércoles, 29 de octubre de 2025 – 10:30 a 12:00 IST

NICOLÁS CABALLERO: Bienvenidos nuevamente. Estamos a punto de comenzar. Adelante, Gulten.

GULTEN TEPE: Bienvenidos a la reunión del GAC con la ccNSO hoy miércoles 29 de octubre a las 10:30 horario UTC. Por favor, tengan en cuenta que esta sesión está siendo grabada y se rige por los estándares de comportamiento esperado de la ICANN, el código de conducta de los participantes de la ICANN y la política antiacoso de la comunidad de la ICANN.

Durante la sesión, las preguntas o comentarios solamente se leerán en voz alta si están formulados de la manera correcta en el chat. Habrá interpretación en esta sesión a los seis idiomas de Naciones Unidas y portugués. Si desean hacer uso de la palabra, por favor, levanten la mano en la sala de Zoom. Recuerden decir su nombre para los registros y el idioma en el que hablarán en caso de que no sea inglés. Les recordamos que hablen a un ritmo razonable para permitir una interpretación correcta. Le doy la palabra ahora al presidente del GAC, Nicolás Caballero.

NICOLÁS CABALLERO Gracias, Gulten. Bienvenidos nuevamente. Tengo el placer de presentar a mis colegas de la ccNSO. A la presidenta, Alejandra, a mi derecha. Vamos a tener una sesión muy interesante, muy interactiva al estilo de lo que hicimos en Seattle. La idea es que haya una participación activa, que hagan preguntas, que interactúen. No hay ninguna pregunta que sea incorrecta. Vamos a tener como distintas estaciones para trabajar.

Antes de ponerlos en contexto y hacer la presentación sobre criptomonedas y un ejemplo de fraude en las inversiones, que estará a cargo de Gabriel Andrews, del FBI, le voy a dar la palabra a Alejandra, para que haga algunas consideraciones prácticas para que sepamos la dinámica para el trabajo de hoy. Adelante, Alejandra. Bienvenida nuevamente. Tiene la palabra.

ALEJANDRA REYNOSO Gracias, Nico. Siempre es un placer sumarnos aquí, en la reunión con el GAC, probando distintas metodologías con ustedes. Creemos que esto es sumamente productivo. Antes de entrar en los detalles de la actividad creo que sería mejor escuchar la presentación de Gabriel. Cuando él finalice les voy a contar todo lo que vamos a hacer en la siguiente parte. Gracias por la invitación.

NICOLÁS CABALLERO Gracias, Alejandra. Ahora le doy la palabra a Gabe Andrews, del FBI. Adelante, Gabe.

GABRIEL ANDREWS

Gracias, Nico. Gracias, Alejandra. Vamos a comenzar con la siguiente diapositiva. Hoy voy a estar hablando de la categoría principal de delito cibernético que se ha informado al FBI en los últimos años, que corresponde al fraude en las inversiones con criptomonedas. También tiene otro nombre en los medios. Es posible que hayan escuchado ese otro término, pig butchering.

Esto nos sirve como información para nuestras conversaciones. Esto es algo que surgió durante la pandemia. Hubo varias consecuencias de la pandemia. Lo que ocurrió es que había bandas del crimen organizado en el sudeste asiático que comenzaron a operar en hoteles con casino en la región y empezaron a aplicar métodos que explotaron como actividad para ganar dinero. Tenían trabajadores que luego quedaban cautivos como esclavos y eran obligados a estafar a personas occidentales a través de esquemas fraudulentos. Es muy importante conocer que existen estos sistemas para lo que les voy a contar luego.

Vamos a cubrir alguno de los titulares que estuvieron en las noticias en los últimos tiempos. En mayo de este año en Naciones Unidas se hizo este informe para poner de relieve la importancia de estos esquemas de fraude para que todo el mundo estuviera al tanto de ello. En los últimos siete días, el ejército de Myanmar pudo atacar uno de estos lugares donde se cometen estas actividades criminales.

También SpaceX comenzó a interrumpir los servicios de Starlink a estos campamentos donde se hacen estas estafas y mi propio Departamento de Justicia en Estados Unidos secuestró también 15.000 millones en moneda de Bitcoin de uno de los esquemas de estafas que era el que correspondía a Prince Group.

Esto no solamente involucra al FBI sino al departamento de justicia de Estados Unidos. La manera en que esto funciona es la siguiente. Hay una actividad de phishing que comienza al principio de la estafa pero no se hace a través del correo electrónico. En cambio, lo que normalmente uno va a ver, es un mensaje en las redes sociales o en las aplicaciones de texto que parece un mensaje accidental que envió alguien. Ni comienza una conversación. Les pueden preguntar si están interesados en una relación de amistad o romántica o tal vez una relación de negocios.

Comienza de manera muy sutil pero este componente de trabajo esclavo permite que quienes cometen phishing se tomen el tiempo para generar esa afinidad con quien recibe los mensajes. Para cuando transforman la conversación en una posibilidad de invertir, en una oportunidad de criptomoneda interesante y nueva, ya ha ocurrido toda una fase de construcción de confianza y de afinidad. Esto es diferente al phishing tradicional que veíamos antes, donde tal vez había un correo muy bien armado. En este caso es un proceso lento de phishing que lleva días o incluso semanas y solamente se puede dar porque estas personas están siendo

cautivas y están obligadas a formar parte del trabajo esclavo. Así permanecen.

El componente de los dominios, porque ustedes se preguntarán: "Si no hay un correo, ¿cuál es el componente de los dominios que está involucrado aquí?" Cuando se establece esta trampa de phishing y los criminales dicen: "Bueno, tuve este retorno sobre mi inversión fantástico. Quisiera compartir esta oportunidad con usted", lo que les van a dar aquí a través de estos mensajes de chat es esta información de las bolsas en las que se comercializan las criptomonedas.

Estos criminales registran en gran volumen. Cuando hablamos de las registraciones masivas justamente este es uno de los ejemplos. A veces pueden registrar cientos o miles de dominios que corresponden a estas bolsas de criptomonedas. Cuando arman esta estructura, esto lo tomé de otra presentación pero para explicarles, lo que va a ocurrir, a la izquierda aquí, en estos rectángulos en púrpura y en amarillo y en rosa comienzan recolectando estos dominios parecidos por los que pueden pasar, que duran tres meses. Pueden pasar al siguiente de ese tiempo.

Como tienen tantos dominios entre los que elegir, pueden ir haciendo ese salto, pero utilizan una técnica que se llama en inglés: CNAME forwarding. Es donde cambian las configuraciones de los nombres canónicos en estos nombres de dominio. Lo dirigen al siguiente dominio el nombre y luego al otro hasta poder llegar al sitio de criptomonedas al final.

Esto permite que el nombre del dominio similar aparezca en el navegador pero pasa por distintos pasos antes de llegar a la resolución. No espero que todos estén al tanto de la configuración de los nombres canónicos CNAME pero algunos tal vez conozcan de esto, sobre todo si operan ccTLD. Tienen que estar al tanto de esta táctica. Si se la encuentran, la van a poder reconocer.

Cuando los investigadores quieren investigar esta situación se dan cuenta de que es difícil explorar la infraestructura justamente por esta táctica. La utilizan por dos motivos: porque les dificultan la investigación a las autoridades y a su vez pueden pasar por estos dominios registrados en gran volumen manteniendo una cierta protección en la infraestructura que está detrás de todo este esquema.

Para ponerlos en contexto para la actividad que van a hacer hoy, lo que quería era plantearles este sistema de estafas, para que estén familiarizados pero también pedirles a los colegas de la ccNSO que nos digan si lo han visto en su espacio, dentro de los gTLD .COM, .INFO, .TOP, .NET. Se ha utilizado este tipo de estafas pero no puedo decir con comodidad que tenemos mucha visibilidad de esto y tal vez es posible que esté ocurriendo en el espacio de los ccTLD. Hay distintas organizaciones que están utilizando este sistema.

La pregunta: ¿Ustedes ven estos informes que tienen que ver con registraciones masivas de sitios de criptomonedas o tal vez tienen este reenvío del CNAME? Para las conversaciones que vamos a

mantener sobre las posibles políticas que se podrían formular con la ICANN en el espacio de los ccTLD, tal vez podríamos considerar algún tipo de verificación de los dominios asociados. Es decir, si tenemos un informe sobre un idioma, tal vez tendríamos que ver qué ocurre con los otros dominios que han sido registrados al mismo tiempo para ver si también forman parte de la estafa o establecer distintos controles a través de las API para poder ver qué pasa con estas registraciones masivas. Creo que de esta manera podríamos tener esta información para la formulación de políticas.

Creo que, según mi cronómetro, ya pasaron ocho minutos. Les agradezco por la atención. Hay muchas respuestas que se están tratando de dar a este tipo de estafas. Con gusto voy a participar en la conversación sobre esto. Gracias.

NICOLÁS CABALLERO: Gracias, Gabe. Ha sido muy interesante. Aquí tenemos las preguntas. Esto es sumamente importante para los operadores del ccTLD. ¿Están recibiendo informes de uso indebido sobre este tema? ¿Están viendo registraciones masivas más al reenvío de los CNAME, de los nombres canónicos? Esta es la primera pregunta.

Ahora le voy a dar la palabra a Alejandra, que nos va a mostrar los detalles y los matices de la actividad que vamos a hacer en los próximos 75 minutos. Le doy la palabra, Alejandra.

ALEJANDRA REYNOSO

Gracias, Nico. Gracias, Gabriel, por la presentación. Sé que tenía tiempo limitado. Vamos a tener en cuenta sus preguntas y le vamos a dar una respuesta luego. En la próxima actividad, como hicimos antes, vamos a tener más interacción. Va a ser una experiencia en la que tengan que estar de hecho de pie. Vamos a hablar del uso indebido del DNS con distintos temas, con personas del GAC y algunos colegas de la ccNSO.

Por ejemplo, en la primera estación tenemos el uso de la inteligencia artificial en la detección y prevención del uso indebido. En la segunda estación tenemos los desafíos de las registraciones masivas, justamente lo que estaba mencionando Gabe. En la sección tres tenemos la investigación del uso indebido con las carteras de nombres de dominios. En la estación cuatro tenemos los marcos nacionales para la prevención de fraude y estafas. En la estación cinco tenemos los acuerdos de notificadores de confianza.

Lo que les pedimos es que tomando la devolución de la última vez, ustedes nos pidieron que tuviéramos más rondas pero eso significaría que tendríamos menos tiempo por rondas. Esta vez vamos a tener tres rondas. En cada ronda ustedes pueden elegir la estación a la que quieren ir. Cuando se termine el tiempo, cambian de estación a la que quieran ir. Si tenemos cinco estaciones, habrá tres oportunidades para interactuar en esas estaciones.

También vamos a incluir luego un resumen de cada estación para que todos tengan la posibilidad de tener toda la información si no

han podido ir a alguna de estas estaciones. Aquí están los nombres de las estaciones. Lo vamos a mantener aquí en la pantalla para que ustedes puedan ir desplazándose. ¿Cómo controlamos el tiempo aquí? Vamos a poner un cronograma aquí a la vista. Muy bien. Nico.

NICOLÁS CABALLERO Gracias, Alejandra. Antes de comenzar con el trabajo en las estaciones, rotando por ellas, quiero volver a la pregunta de Gabe. Me gustaría tener alguna respuesta de aquellos que están conectados por Zoom o quienes están aquí, a estas preguntas. Déjenme dedicar tres o cinco minutos a esto antes de que comencemos con el trabajo en las estaciones, con todo el campeonato de pesos pesados del uso indebido del DNS.

¿Alguna devolución, alguna respuesta, sobre todo de los operadores de los ccTLD con respecto al tema del reenvío de CNAME de estos nombres canónicos? Nuevamente, no esperamos que todos sean expertos en estos saltos del DNS o en los reenvíos de estos registros CNAME. Alejandra.

ALEJANDRA REYNOSO Para comenzar esta conversación quisiera dirigirme con una pregunta a la ccNSO. Si consideraríamos desarrollar una política para esto. Quiero reiterar que la ccNSO tiene un ámbito de competencia muy limitado con respecto al desarrollo de políticas que tiene que ver con la IANA y lo que se necesita para administrar

los ccTLD. Por ejemplo, el retiro, la transferencia de ccTLD. Este tipo de operaciones dentro del marco de la IANA.

No podemos desarrollar políticas para decirles a los ccTLD cómo tienen que hacer su trabajo. Sin embargo, tenemos un Comité Permanente sobre el uso indebido del DNS que ha tenido un papel muy importante para organizar esta sesión con todos ustedes. Allí tenemos un repositorio de buenas prácticas que vamos recabando para compartirlas con todo el mundo con respecto a cómo los ccTLD lo están manejando y creo que esta actividad que vamos a hacer puede ampliar la conversación un poquito más. No veo ninguna mano levantada por ahora.

NICOLÁS CABALLERO Gracias por esta respuesta, Alejandra. Denme un minuto más para responder a la segunda pregunta. Con respecto a las experiencias que puedan tener los operadores de ccTLD o no para poder dar información para el desarrollo de esas políticas.

No veo ninguna mano aquí, en la sala, ni tampoco ninguna mano en línea. Le devuelvo la palabra. Gracias nuevamente, Gabe. Si todavía está en línea, muchísimas gracias. Estoy muy importante y ciertamente es pertinente para todos los representantes del GAC. Gracias por esta presentación. Alejandra.

ALEJANDRA REYNOSO Nos llevamos estas preguntas y vamos a devolverle una respuesta a Gabriel. Gracias. Con esto los invito ahora a ponerse de pie e ir a

la estación que prefieran. Yo voy a mantener el cronograma aquí y para esta primera ronda vamos a tener 18 minutos. Comienza ya el tiempo a contar ahora.

Hola a todos. Se acabó el tiempo. Les pido, por favor, que terminen la conversación y que cambien de estación. Vamos a dar inicio a un nuevo cronómetro en un minuto.

Vamos a empezar la segunda ronda. Por favor, cambien de estación. Trasládense de una estación a la otra y demos inicio al cronómetro, por favor.

Quiero alertarlos de que faltan solamente dos minutos.

Se acabó el tiempo. Les pido, por favor, que vayan cerrando y pasen a otra estación para la tercera ronda. En un minuto vamos a dar por iniciado el cronómetro. Espero que hayan llegado a la tercera estación. Ahora comenzamos a hacer correr el cronómetro.

Quedan dos minutos. Se acabó el tiempo. Por favor, vuelvan a tomar sus asientos. Les pido por favor que los redactores y los líderes vuelvan también a su asiento porque vamos a tratar de hacer un resumen de la actividad realizada. Unos segundos más, por favor, para que todos tomen asiento y comencemos con los resúmenes.

Vamos a tener un micrófono volante, que va a ir de una estación a otra. Vamos a empezar entonces con el uso de la inteligencia artificial y detección de uso indebido y prevención.

NICOLÁS CABALLERO

En lo que tiene que ver con el uso de inteligencia artificial y el aprendizaje automático, en primer lugar explicamos con Christian, de .NL, realmente fueron tres rondas o minisesiones de IA con ML, que es la inteligencia artificial. La diferencia entre ChatGPT, etc. Lo que tiene que ver con la inteligencia artificial generativa, el aprendizaje automático. Estuvimos hablando también del tráfico del DNS, de cómo se utilizan los algoritmos para detectar amenazas en el DNS. Estuvimos hablando de las distintas diferencias. Utilizar una cosa que puede ser inteligencia artificial generativa.

En este caso, el equipo de Países Bajos está implementando para combatir el uso indebido del DNS muchas cosas interesantes sobre las medidas que están adoptando. También lo que tiene que ver con la implementación, la mecánica interna, de qué forma. Todo esto está trabajando en el ámbito interno. Qué es lo que sucede por debajo de la capa general.

Creo que fue muy interesante y espero también que les haya gustado a los participantes. Muchísimas gracias nuevamente, Chris y al equipo de .NL. Esto es el mini informe que les puedo dar de la estación número uno.

ALEJANDRA REYNOSO Ahora vamos a la estación número dos, que son los desafíos de las registraciones de dominios masivas con Peter Koch y Martina Barbero.

PETER KOCH Nosotros estuvimos hablando de la registración masiva. No hablamos de la definición de lo que es la registración pero estuvimos hablando de por qué esto es un desafío por un lado pero, por otro lado, no es tan importante. También estuvimos discutiendo la registración automática, hacer una diferencia entre la comunicación entre un registrador y un registro, en comparación con la automatización del registro para otros y dónde puede haber quizá algo potencial como para seguir investigando sobre eso. Ahora le doy el micrófono a Martina.

MARTINA BARBERO Fue muy interesante la discusión. Hubo muchas preguntas muy buenas pero básicamente estuvimos hablando de la forma en que abordar las inquietudes que tienen que ver con la registración masiva. Hablamos de la tensión entre tratar de entender cuál podría ser la intención detrás de estas registraciones masivas y cómo puede utilizar, por ejemplo, una marca que hace un registro masivo de múltiples marcas, entonces esto puede ser legítimo mientras que por el otro lado tratar de definir cuáles son los usos ilegítimos para poder desalentarlos.

También cuando hablamos de identificación estuvimos hablando de la diferencia entre identificar organizaciones y personas que exige distintas prácticas y enfoques. También hablamos de distintas prácticas desde el espacio de ccTLD. Algunos registros sí analizan las conductas que pueden ser sospechosas después de la delegación, tratar de reconocerlas, tratar de enfrentarlas en algunos casos que son registraciones masivas y otros casos que tienen que ver con esas conductas sospechosas antes de la delegación en sí misma.

También estuvimos hablando de la importancia de ser conscientes de la cantidad de daño que puede realizarse en poco tiempo con campañas de phishing como escuchamos de nuestro colega Gabriel anteriormente y también la reactividad del plazo que tiene que ver con las intenciones como para ser veloz. Esta es una limitación. Tenemos que tener en cuenta cuando hablamos de los remedios. No hay demasiadas ideas brillantes como para solucionar esto inmediata pero creo que fue muy útil la deliberación.

ALEJANDRA REYNOSO Ahora vamos a la estación número tres que tenemos aquí. Hemos investigado el uso indebido dentro de las carteras de dominios con Crystal y Susan Chalmers.

SUSAN CHALMERS

Susan Chalmers, representante de Estados Unidos y NTIA, que es la autoridad de políticas para el dominio de alto nivel con código de país de .US. Estuvimos aquí con Crystal Peterson, que está en los servicios de registro que administran el ccTLD de .US.

Ahora voy a compartir algunos puntos con ustedes y después le voy a dar la palabra a Crystal. Nosotros en nuestra estación estuvimos hablando de lo que se va a ver en el próximo proceso de desarrollo de políticas, que son las verificaciones de dominios, que es cuando hay un informe de uso indebido. El registro de TLD de .US es el recurso autoritativo que tiene que ver con la zona raíz de .US y tiene la información del registratario.

En este caso, por política se prohíbe el uso de los servicios de privacidad y representación. Tenemos los datos en la base de datos como datos del registratario que nos ponen a nosotros en una posición única como para poder mitigar el uso indebido sobre la base del aporte que recibimos. Crystal, le voy a dar la palabra ahora.

CRYSTAL PETERSON

Gracias, Susan. Lo que vimos durante las tres sesiones, estuvimos reviendo de qué forma nosotros, como registro, podemos detectar dominios asociados y carteras de dominios. Esto nos vuelve a una de las preguntas que tuvo Gabe al principio de nuestra sesión sobre el fraude con criptomonedas.

Como Estados Unidos tiene unas políticas únicas porque no hay servicios de privacidad ni de representación, nosotros tenemos entonces también la verificación de los datos del WHOIS y lo vemos desde una perspectiva de registro, para poder ayudar en los esfuerzos de mitigación del uso indebido que hace la comunidad para poder identificar dominios asociados a través de los datos de contacto de los registratarios. Nuestra sesión fue muy buena porque pudimos rever de qué forma definimos dominios asociados, qué es lo que estamos mirando desde la perspectiva de mitigación y hubo muy buenas preguntas planteadas.

ALEJANDRA REYNOSO Muchísimas gracias. Vamos a pasar ahora a la estación número cuatro, que es marcos nacionales para la prevención del fraude y las estafas. Tenemos ahí a Bruce Tonkin y a Ian Sheldon.

IAN SHELDON En la estación número cuatro tuvimos una discusión fantástica sobre los marcos para combatir las estafas. Hay algunos pasos que se necesitan hacer en los ámbitos nacionales, sobre todo en lo que tiene que ver con la prevención, disrupción, respuesta y después también enviar la información a las partes pertinentes.

Nosotros en Australia tenemos un centro antiestafas nacional que está encargado de abordar estos temas. Digamos que es la puerta de entrada para la población general, para que puedan informar y denunciar cualquier tipo de estafa y encontrar alguna solución.

Trabajan en conjunto con .AU, el operador de ccTLD. Hay muchas acciones de respuesta cuando se alerta sobre una estafa.

Tuvimos un buen intercambio sobre cuántas estafas tienen que ver con ciberseguridad, cuántas tienen que ver con un problema de protección al consumidor. En Australia, el centro nacional que mencioné tiene una comisión de competencia para el consumidor y lo toma como una cuestión que tiene que ver con la protección del consumidor. Hay igual una interacción con el equipo de ciberseguridad pero hay otras medidas que se pueden tomar para garantizar la protección a los consumidores.

Tuvimos una buena discusión sobre los requisitos que tenemos para tratar de reducir estos problemas aunque no quizá eliminarlos pero sí hablar de todo lo que tiene que ver con los requisitos, las credenciales. Si uno tiene los requisitos implementados en su lugar, esto puede ser aún mejor. También con el requisito de nexo. No sé si Bruce tiene algo para agregar. Si no, esto es todo.

ALEJANDRA REYNOSO Entonces vamos a pasar con los acuerdos con notificadores confiables. Tenemos entonces a Vincet y a Tomonori Miyamoto.

JAKE VINCET Estuvimos hablando de las distintas capas que puede haber y cómo puede haber obstáculos también para los acuerdos con notificadores confiables. Por las personas que visitaron nuestra

estación, significa que a veces no son tan populares estos notificadores confiables. Este es uno de los desafíos que podíamos tener también con las jurisdicciones extranjeras. Cómo se sabe que estos informes son exactos. Algunos pueden ver los beneficios de este tipo de acuerdos. .UK tiene algunos. Con esto termino.

ALEJANDRA REYNOSO Gracias a todos. Voy a tratar de empezar a dar cierre a esta sesión pero me gustaría que la calificaran. Querríamos escuchar sus comentarios y, si les parece que el resumen no fue suficiente, no se hagan problema porque vamos a enviar un resumen con todo lo debatido en cada una de las estaciones para el GAC, para que ustedes tengan toda la información lista y a mano. Ahora le doy la palabra a Nico.

NICOLÁS CABALLERO Gracias. Gracias, Alejandra. Gracias a la ccNSO porque realmente ha sido una sesión fantástica. Es una de mis favoritas, obviamente con el debido respeto al resto de las unidades constitutivas.

Creo que tenemos que hacer más sesiones como esta con las otras unidades constitutivas también, porque son interactivas. Hay mucho intercambio de opiniones entre unos y otros. Muchísimas gracias a la ccNSO.

Es muy importante para ustedes que completen el Mentimeter. Les puede llevar unos minutos. Les pido por favor completar la encuesta. Esto nos va a ayudar a decidir, por ejemplo, si el tiempo

asignado a cada una de las rondas es suficiente, si fue demasiado, si fue muy breve. Tienen que ser 20 minutos, tienen que ser 15. Más tiempo para el cierre, etc.

Muchísimas gracias por todo. Con esto terminamos con la sesión. Nos pasamos cuatro minutos pero ahora quiero hablar de algunos temas para los que estamos aquí. Tenemos almuerzo y van a tener 15 minutos adicionales porque tenemos una reunión de los líderes de la ICANN. Tienen que regresar a las 13:30 en lugar de a las 13:15.

ROBERT HOGGARTH 13.45.

NICOLÁS CABALLERO Mejor. 13:45. ¿Alguien se opone? ¿Alguien se opone realmente? Este es el momento de hablar. Muchísimas gracias a todos. Con esto terminamos la sesión y les pido que regresen a las 13:45. Un gran aplauso, por favor, a los colegas de la ccNSO.

ALEJANDRA REYNOSO Muchas gracias.

[FIN DE LA TRANSCRIPCIÓN]