ICANN83 | Foro sobre políticas – ccNSO: DASC Online, estafas y delitos financieros
Miércoles, 11 de junio de 2025 – 13:45 a 15:00 CEST

CLAUDIA RUÍZ

Hola y bienvenidos a esta sesión de la ccNSO DASC de delitos financieros, con mis colegas seremos los coordinadores de participación remota de esta sesión, por favor tengan en cuenta que esta sesión se está grabando y se rige por los estándares de comportamiento esperados de la ICANN, y la política antiacoso de la comunidad.

En esta sesión las preguntas o comentarios que aparezcan en el chat se leerán en voz alta, si se presentan en el recuadro adecuado que se indica en el chat. En esta sesión habrá interpretación para inglés, francés y español, si quieren tomar la palabra durante la sesión, por favor, levanten la mano en Zoom, cuando se diga su nombre los participantes virtuales podrán activar sus micrófonos en Zoom y los participantes presenciales utilizaran los micrófonos de la sala para hablar, por favor digan su nombre para los registros y el idioma en el que hablarán, y hablen a una velocidad razonable para que la interpretación pueda ser precisa. Muchas gracias y dicho esto, le doy la palabra a Nick Wenban-Smith.

NICK WENBAN-SMITH

Gracias, Claudia. En primer lugar, soy de NOMINET .UK ccTLD, soy presidente del comité permanente de uso indebido del DNS de la ccNSO. Esta sesión va a ser una sesión muy interesante y ha sido preparada tomando en cuenta lo que se hizo en reuniones anteriores, pensando en lo que queremos analizar en mayor detalle, cuáles son las prioridades para los ccTLD de todo el mundo, así que, es un placer realmente presidir este panel de expertos que seguramente compartirán contenido muy interesante con nosotros, la idea es que la sesión sea interactiva, así que, queremos recibir preguntas, voy a controlar lo que vaya pasando en Zoom, pero el personal de la ICANN seguramente me ayudará aquí.

Tenemos una agenda bastante completa, así que, voy a presentar brevemente a los panelistas, vamos a empezar según como aparecen en pantalla. Gabriel.

GABRIEL ANDREWS

Soy Gabriel Andrews, soy copresidente del grupo de trabajo de seguridad pública en la ICANN y durante el día trabajo para el FBI en los Estados Unidos.

NICK WENBAN-SMITH

Gracias, Gabriel. Ahora Keith.

KEITH DRAZEK

Buenas tardes, soy Keith, trabajo para VeriSign y estoy a cargo dentro de la empresa del programa de mitigación del uso indebido

	del DNS, además, dirijo el equipo de políticas de la ICANN, es un placer estar aquí en la ccNSO. Algunos recordarán que yo antes trabajaba para otra empresa, trabajaba dando soporte al .US. Gracias.
NICK WENBAN-SMITH	Mon, ¿me escucha? ¿Podría activar su micrófono y presentarse?
MON PEREZ	Soy Mon, soy administrador técnico de las operaciones de registro y nombres de dominios .SG, también estoy desarrollando un sistema de gestión de uso indebido de DNS. Muchas gracias.
BRUCE TONKIN	Soy Bruce Tonkin del código de país .AU.
NICK WENBAN-SMITH	Muchas gracias y especialmente a Mon por quedarse levantado a esta hora tan poco cómoda en Singapur. Como pueden ver, en la diapositiva, la mayor parte de las fotografías de los panelistas son de antes del COVID-19, además, de Mon que no tiene este tipo de fotos. Para hacer una breve introducción quiero decirles que esta sesión empieza con una exploración del tema de fraude financiero, estafas en línea y la intersección con el uso de nombres de dominios para cometer estos delitos, los sus indebidos del punto de vista técnico y el impacto que esto tiene en la sociedad, o sea

estamos viendo más bien la escala del problema y después alguna presentación sobre abordajes y desafíos pendientes.

Esto es lo que hace el DASC, el comité permanente de uso indebido del DNS. Quiero decirles que no estamos aquí para desarrollar políticas para los ccTLD, eso se hace a nivel nacional de cada país, pero estamos aquí para socializar, hablar de los temas pendientes, crear mayor consciencia, la idea es que haya un dialogo abierto y constructivo, pero por supuesto, en última instancia, estamos interesados básicamente en reducir la cantidad de casos de uso indebido en los registros ccTLD y ayudar a todos a lograr ese objetivo.

Aquí estamos simplemente sentando las bases de lo que vamos a hablar, en 2022 y en 2024 hicimos una encuesta global entre los ccTLD, esta es una palabra legal interesante. En cuanto a las políticas de la ICANN, los gTLD están dentro del ámbito de alcance de las políticas de la ICANN en cuanto a la definición técnica de uso indebido del DNS, pero en estas encuestas vimos que muchos ccTLD no tienen esta distinción entre ciertos tipos de uso indebido y otros.

En general, dicen que uso indebido y los contenidos delictivos, por ejemplo, el fraude es un problema importante y en realidad se puede actuar cuando sucede algo de este tipo y el registro, en general, interviene en esos casos. Quisiera volver a hablar de lo que pasó en Kigali donde los registros de África y los de Nigeria… Los reguladores en especial hablaron sobre la plaga de estafas con

criptomonedas, una enorme cantidad de fraude que tenían lugar y esto afectaba a los consumidores y ciudadanos de esos países.

En el Reino Unido de donde yo provengo el fraude es el 40% de todos los delitos, que es mucho, es el tipo de delito más difundido y el 80% de los fraudes con pagos tienen que ver con las redes sociales o sitios webs falsos, o sea esto realmente está dentro del ámbito de trabajo de muchos registros de ccTLD, pero aquí hay una superposición en cuanto a la definición técnica de uso indebido del DNS que incluye phishing, que es el principal modo de uso indebido y, por supuesto, también el uso de correos electrónicos de phishing como punto de inicio de los delitos financieros.

En Seattle también hablamos sobre este tema, así que, ahora vamos a pasar a los panelistas y pasamos a la próxima diapositiva, pero antes tenemos esta definición. Una estafa es una invitación, solicitud, notificación u ofertas fraudulentas, cuyo objetivo es obtener información personal, dinero u obtener beneficios financieros, en general, pero no siempre a través de dominios registrados en forma maliciosa.

Esta es una sesión introductoria y la idea es que después sigamos trabajando en estos temas en próximas reuniones de la ICANN y pueden ver que ahora tenemos una conversación que involucra a muchas comunidades, tenemos un Mentimeter aquí para esta sesión, así que, podemos avanzar.

Le voy a dar a todos un minuto para conectarse aquí, hay dos formas de conectarse, pueden utilizar el código que ven en

pantalla, esto lo hacemos muy bien en la ccNSO, usamos estas encuestas interactivas, esto ayuda a aquellas personas cuyo idioma nativo no es el inglés, que son la mayor parte de los ccNSO aquí.

Entonces vamos a la pregunta si ya todos pudieron conectarse. Es una pregunta sencilla, ¿en qué medida su registro está bien preparado para detectar uso indebido de dominios relacionados con delitos financieros? Les dejamos la posibilidad de responder.

Esta no es una encuesta científica exacta, simplemente es para ver qué opinan y cuál es la escala del problema, entonces dicho esto, quiero darle la palabra a Gabriel para que comparta su presentación. Gabriel, le damos la palabra.

GABRIEL ANDREWS

En Seattle hablé con Nick y dije que había un informe de delitos informáticos que publica el FBI todos los años y que se publicó un poco después de Seattle, él dijo que quería ver la información aquí, así que, quiero aprovechar la oportunidad.

Estos datos provienen del portal de denuncias de delitos informáticos, cuando una víctima viene a nosotros y nos dice que sufrió un delito, lo registramos para justificar los recursos que invertimos en todo este trabajo, pero, además, así obtenemos estadísticas que se publican una vez por año.

Quiero reconocer que soy simplemente una autoridad de un solo país, pero recibimos, en realidad, denuncias de más de 200 países

del mundo, por lo menos así fue en 2024. Desde Reino Unido se presentaron más de 100.000 denuncias, esto refleja el hecho que el ciberdelito es algo global y yo, creo que, aunque estoy hablando de estadísticas de Estados Unidos, esto representa muy bien lo que están viendo mis contrapartes en todo el mundo.

Entonces, ¿qué hacemos? Nosotros contamos cuantas denuncias recibimos y después también tratamos de ver cuáles son las pérdidas asociadas con cada tipo de delito. Aquí tengo subrayados algunos, espero que los puedan ver a la izquierda. Cuando vemos el tipo de delito pueden ver que el phishing representa la mayor cantidad de delitos cometidos y sabemos que el phishing tiene lugar continuamente.

Como dijo Nick, es el punto de inicio para realizar después otros delitos y si vamos hacia la derecha y tratamos de ver dónde se dan las pérdidas, la principal categoría es fraude relacionado con inversiones, fraude en inversiones con criptomonedas y Nigeria mencionó esto, dijo que era una plaga y lo es, ya que representó más de $6.5 billones en pérdidas el año 2024 en Estados Unidos y también causa una gran cantidad de suicidios, después vamos a hablar de esto.

Ahora quiero hablar un poco del correo electrónico corporativo comprometido, que es otro tipo de phishing, y después voy a hablar de Ransomware porque a pesar de que está abajo en la lista y son solo $12 millones en pérdida, es un tipo de fraude. Vamos a hablar ahora del correo electrónico corporativo comprometido.

Empezamos con phishing donde una persona asume falsamente la personalidad de otra, un CEO, por ejemplo, para iniciar una transferencia de fondos y esto es un correo electrónico que parece natural, obtuvimos permiso de esta empresa para usar estos email con fines educativos. Próxima diapositiva por favor.

Pueden ver que el tema aquí estaba suplantando la personalidad de otra empresa y como investigador lo primero que hago, es decir: "¿Qué información tenemos disponible sobre este nombre de dominio? ¿A quién le pertenece?" Entonces entro en WHOIS y en ese momento vería esta información, entonces yo miré esto y dije: "¿Con quién puedo iniciar este proceso legal? ¿Esta empresa o persona está en mi país o en otro país? ¿Dónde tenemos que investigar esto?" Próxima diapositiva.

Iniciar un proceso legal lleva un tiempo, después de dos o tres semanas ya tengo la orden judicial, envío, recibo los resultados, entonces quizás haya pedido lo siguiente: ¿Cuáles son los otros nombres de dominios que este delincuente ha registrado además de este que está tratando de llevar a cabo un delito?

Quizás haya 12 o 24 nombres de dominios que se registraron y utilizando mi cerebro de investigador puedo ver cuáles son los nombres de dominios parecidos y mientras hago esta investigación también quiero notificar las posibles víctimas que están siendo identificadas y que las está tratando de atacar un delincuente, entonces no tengo tiempo para pasar un proceso legal con cada uno de los registradores a cargo de esos dominios, pero si

encuentro algunos números de teléfonos en WHOIS sobre estas posibles víctimas, quizás pueda evitar que haya otros perjuicios.

De manera muy similar con la Ransomware, yo hablé con mi agencia hermana CISA, que es responsable de la protección de infraestructura crítica en Estados Unidos y quiero subrayar que esta es otra categoría de delito totalmente diferente, en su misión este organismo hace algo parecido a lo que yo acabo de escribir, ellos también están en un posición de tratar de evitar daños y perjuicios.

En este caso, tenemos investigadores en ciberseguridad que están viendo qué pasa con estos servicios, saben que cuando aparece una nueva víctima que se conecta con la infraestructura de Ransomware, en las siguientes, 24, 48 o 72 horas quizás haya un Ransomware instalado en la red de la víctima, después de eso se activará y causará perjuicios.

Entonces los investigadores nos avisan sobre esto, contactan a CISA, al FBI y nos dicen: “Aquí hay un IP víctima de un ataque de Ransomware”, entonces CISA tiene el reloj, tiene que ver con qué velocidad puede identificar a la posible victima para iniciar una conversación.

Entonces realmente necesitan registros públicos para transformar esos identificadores de IP en información del mundo real, es muy importante poder contar con esta información, ya se hicieron más de $8.5 millones de pagos en Ransomware el año pasado.

Estoy tratando de ver esto rápidamente porque tenemos poco tiempo. Fraude por inversiones en criptomonedas, aparentemente ya se habló de esto en Nigeria, en Estados Unidos es la categoría de pérdidas más alta con $6.5 millones, creo que, todos los que están aquí seguramente ya recibieron uno de estos posibles ataques.

Todo empieza con un mensaje de WhatsApp u otra plataforma de chat y siempre inician amigablemente, alguien quiere iniciar una conversación con nosotros, dicen que conocen a tu médico, a tu dentista, a un amigo o lo que fuera y que simplemente se conectaron con ustedes por error.

Finalmente, desarrollan una conversación para crear confianza y después les empiezan a decir: “Gané tanto dinero con esta plataforma de criptomonedas”. Si empiezan a entrar en esto en algún momento, empezarán a invertir ustedes mismos porque escucharon que esta persona ganó mucho dinero y van a invertir cada vez más de sus ahorros en esto, esto pasa muchas veces.

Cuando hacen esto presentan una plataforma de bolsa de criptomonedas falsas que parece muy real y auténtica para las víctimas. Cuando yo hablo de los agentes que investigan estos casos… Me dicen que los delincuentes están muy bien preparados, registran cientos de dominios maliciosos a fin de promover estas bolsas falsas de criptomonedas, entonces si ustedes están observando que están haciendo registraciones masivas a través de un ccTLD, incluso aunque los dominios en sí mismos no sean ccTLD, se van a utilizar los ccTLD para cometer este tipo de delitos.

El volumen que tienen les permite promover estas bolsas, entonces si se retira un dominio pasan al siguiente y la parte difícil aquí es que cuando los investigadores analizan estos casos, muchas veces los registradores que se están utilizando no están ubicados en el mismo país que en el que están las autoridades de aplicación de la ley y esto causa algunos otros problemas. Próxima diapositiva, por favor.

Cuando utilizamos información disponible públicamente como se ve aquí en esta gráfica como Google u otros recursos, nosotros en segundos o minutos podemos verificar esto y como policías nosotros tenemos la autoridad de mandar citatorios judiciales, fallos u órdenes judiciales, pero cuando eso cruza fronteras internacionales solo nos podemos basar en herramientas disponibles para nosotros como, por ejemplo, solicitudes de tratado de asistencia legal mutua y eso a veces toma 6 a 12 meses cuando lo he hecho anteriormente.

Entonces eso no contribuye a investigaciones rápidas, el punto es que cuando nosotros logramos voluntariamente aceptar cosas como datos, WHOIS o los operadores de ccTLD, cuando no estamos en el mismo país eso ayuda que rápidamente nosotros nos enteremos de estos delincuentes.

Un resumen breve de los puntos ya mencionados, WHOIS ayuda mucho a los policías cuando estamos tratando de averiguar acerca de dónde mandar estas órdenes judiciales o procesos legales a los lugares adecuados.

Por favor hagan una lista si usted mismo utiliza estos revendedores, las agencias de seguridad pública quieren utilizar WHOIS para evitar daño a las víctimas, también fraude de inversión de criptomoneda es muy malo porque requiere registros de sitios webs en cantidades masivas y, finalmente, investigaciones cruzando fronteras a veces es muy lento, entonces por eso pedimos que, si puede divulgar información voluntaria a su discreción, eso nos ayuda.

Gracias por su atención, espero que esto haya sido de interés y estoy agradecido por la oportunidad que me dieron para hablar en la sesión. Le doy la palabra a Nick.

NICK WENBAN-SMITH

Gracias, Gabriel. Lo único que yo iba a decir es que muchos de los ejemplos parecen que son detallados para gTLD, pero sí aplica ccTLD. Mi perspectiva, con todo respeto, no reconozco la autoridad de Estados Unidos, pero si yo recibo alguna información del FBI se va a tomar en cuenta, especialmente cuando tiene que ver con políticas internas para cada ccTLD.

Si nosotros vemos, por ejemplo, que hay datos de registración falsos, entonces hay procesos más rápidos que muchos registros responsables podrían voluntariamente ayudar, pero bueno, sigamos con Keith, que está a mi izquierda.

KEITH DRAZEK

Muchas gracias, Nick. Hola a todos, estoy aquí para darles una introducción a una nueva iniciativa, que se llama el foro de infraestructura de internet, IIF, quiero darles un contexto y un historial con respecto a por qué esto es algo que nosotros estamos apoyando junto con otros foros u otros organismos.

En el 2022 los registros y registradores de gTLD nos dimos cuenta de que tenemos que tomar la iniciativa de lidiar con el tema del uso indebido del DNS como se habló en el espacio de la ICANN, ustedes saben que los registros y registradores de gTLD tienen contrato con la ICANN, ha sido una conversación de 10 años en lo que tiene que ver con el tema del uso indebido del DNS y reconocemos que algo se tenía que hacer.

Entonces nosotros voluntariamente participamos junto con la ICANN esencialmente ofreciendo y pidiendo aceptar obligaciones nuevas que se tienen que cumplir a nivel contractual y como parte del proceso definimos el uso indebido del DNS con la ICANN en nuestros contratos que tiene que ver con phishing, pharming, malware, botnets y estafas.

Entonces el tener este término definido con respecto al uso indebido del DNS, también nos dimos cuenta de que iba a existir una presión continua de parte de la ICANN de participar en daños relacionados con contenido, para ustedes que no están familiarizados con esto.

Los estatutos de la ICANN prohíben que nosotros nos involucremos con el cambio de contenido, entonces nos dimos cuenta de que

teníamos que desarrollar otro punto de participación para múltiples partes interesadas que incluya el aspecto del contenido, pero que ocurra externamente a la esfera de la ICANN.

Entonces en paralelo a estas discusiones con respecto a negociaciones del contrato, los registradores y registros del gTLD se reunieron y empezaron a hablar acerca de la necesidad de desarrollar lo que ahora se llama el foro de infraestructura de internet.

VeriSign, PIR, Identity Digital, Google, Amazon y CloudFlare fueron las seis empresas que se unieron, se dieron cuenta que vale la pena seguir con este proceso y queríamos que los operadores de infraestructura de internet participaran en el contenido, los CDN, etc., que todos se reunieran y empezáramos a hablar de cómo nosotros como operadores de infraestructura de internet pudiéramos trabajar en conjunto y mitigar estos daños en línea de una manera más amplia de lo que se define dentro del espacio de la ICANN.

Esto fue una iniciativa que comenzó el año pasado, tuvimos nuestra primera reunión presencial la primera semana de febrero en Ámsterdam este año, tuvimos 53 participantes representando a 38 organizaciones, a través de una reunión de dos días, se recibió positivamente esencialmente las seis empresas, iniciamos esto y trabajamos cercanamente con la red de política de jurisdicción de internet.

Quiero darle reconocimiento a Bertrand LA Chapelle que está aquí con nosotros hoy, él es el coordinador líder y el facilitador para este tipo de esfuerzo para el foro de infraestructura de internet, también trabajamos con ICO, que es la iniciativa mayor del DNS, y también la coalición de infraestructura de internet I2C en Norteamérica.

Entonces el grupo de facilitadores está trabajando en hacer que estas metas del IIF avancen. Ahora, de la reunión de Ámsterdam surgió que fue muy importante para nosotros validar que esto es un esfuerzo que vale la pena, especialmente entre los alojadores web y quienes no necesariamente participan en el espacio de ICANN a no ser que tuvieran un registro o un registrador para que participen en estas conversaciones, queríamos validar que existiera un interés, una disponibilidad de querer participar para que trabajemos juntos de una manera colaboradora y compartir información, identificar temas concretos para ayudar a mitigar datos en línea que pudieran ocurrir, establecer responsabilidades y capacidades técnicas.

Entonces en la reunión de Ámsterdam identificamos cuatro puntos, unos que se enfocaran en la política legal y desarrollos reglamentarios que incluye implementación de DSA, cuestiones de transparencia, conocer a sus clientes, entonces eso fue un tema que ayudó a informar y a apoyar otros trabajos que están más enfocados en este tema.

El segundo punto tiene que ver con cuestiones de información y automatización, como desarrollar sistemas que facilite la compartición de información, dirigir esta información para que entonces todos puedan comunicar de manera más eficiente y así ayudarnos todos a poder tratar estos daños con más rapidez.

El tercer punto, aunque se enfoca más en CSAM y en NCII, es acerca del rol de los notificadores confiables con respecto a mitigar el uso indebido del ecosistema. Y el último punto de estos cuatro es phishing plus, phishing es uno de los vectores más grandes del fraude, pero habilita otros tipos de fraudes y usos indebidos dentro de esta categoría.

Entonces es una iniciativa emocionante, queremos expandir la participación de otros, pero tenemos que también mantener un equilibrio entre los operadores tradicionales del DNS para asegurarnos de que tengamos un nivel de contenido.

Quiero decir también que esto es una inicial dirigida por la industria donde proveedores de servicios participan para facilitar esta mitigación de estos usos indebidos o estos daños, pero el plan es expandir ese trabajo para asegurarnos de que exista una participación de múltiples partes interesadas para asegurarnos de que nos conectemos con otros grupos interesados y con otros grupos peritos, ese es el próximo paso a tomar y progresar en esto, asegurarnos de que participen múltiples partes interesadas para asegúranos de que estemos bien informados.

NICK WENBAN-SMITH

Gracias, Keith. Presentamos la razón por incluir ese tema, el llegar al alojamiento del sitio web con phishing y evitar ese daño, es la meta. Una interrupción de esta actividad de ccTLD no previene que eso no les ocurra a otros nombres de dominios, ya sea que sean gTLD también.

Entonces es interesante que lo tomemos en cuenta a medida que conversamos más de ese tema, es que tiene que ver con cuestiones relacionadas con contenido, hablemos entonces con Singapur para que nos hable acerca de un estudio de caso y su iniciativa de combatir estos delitos.

MON PEREZ

Gracias, Nick. Sabemos que delitos de ese tipo es un problema mayor porque significa pérdida financiera y también afecta la confianza de los usuarios. Hubo 8.000 intentos de phishing en 2022, afortunadamente ninguno de ellos fue de Singapur, sino de otros lugares, 80% de los intentos de phishing eran de servicios de bancos, gobierno y logística.

A SGNIC le preocupa estos tipos de fraudes, para ponerlos en contexto, estos son los usos indebidos de los que se ha enterado la ICANN, que es el malware, phishing, estafas y pharming. La segunda columna es lo que le preocupa a SGNIC y hablaremos más detalladamente de los que tienen asterisco.

La última columna no es tanto el uso indebido, sino más bien son indicadores que nuestro equipo utiliza para detectar señales tempranas de algún posible delito, estas son medidas preventivas que se utilizan, primero tenemos verifiedID@SG donde se asegura que la registración de nombres de dominios pase por algún tipo de verificación utilizando SINGPASS.

Segundo, tenemos Registry Lock, que es una característica gratis de seguridad donde ayuda a los registratarios de .SG mitigar el riesgo de algún tipo de modificación no autorizado. Y, por último, tenemos un sistema de manejo del uso indebido AMS, que es un sistema interno que monitorea cuando existen cosas maliciosas en los sitios webs y así les da alerta a las partes interesadas.

Voy a indagar un poco más en lo que tiene que ver con el sistema de manejo del uso indebido, básicamente esto se desarrolló internamente y lo que hace es que detecta y rastrea el uso indebido del nombre de dominio, malware y phishing, también verifica algún registro sospechoso indebido y la registración de bots, nos da advertencia de cualquier uso indebido de nombre de dominio posible, tenemos que validarlo y si es un caso confirmado, entonces le notificamos a las partes interesadas, los registratarios y registradores.

Inicialmente SGNIC colaboró con una investigación legal porque en ese entonces no estábamos enterados de cómo detectar esto, pero después tuvimos colaboración para que nosotros pudiéramos incluir esto dentro de nuestro sistema. Esta es la otra característica

del sistema de manejo del uso indebido, básicamente es para detectar cualquier registración incorrecta sospechosa. Hay un número de registración de empresas y el sistema lo verifica con la base de datos de registración de empresas, y en base al nombre de la empresa entonces se hace una verificación cruzada para ver si la registración es maliciosa o sospechosa, o no. La siguiente diapositiva, por favor.

Aquí existe otra parte del AMS, estos son informes que nos dan unas ideas de ataques comunes o aplicaciones en las cuales nos enfocamos y nos muestra cuáles son los usos indebidos comunes, o si hay algún incremento en el uso indebido de nombres de dominios que se hayan detectado. Siguiente diapositiva, por favor.

Entonces, ¿a dónde nos han llevado todos estos esfuerzos? En primer lugar, no se deduce incidente de secuestros de nombres dominios porque tenemos un sistema ahora, entonces podemos medir nuestras tasas de resolución de problemas, nos aseguramos de tener un 80% de los casos resueltos por mes, ese es nuestro objetivo. En tercer lugar, estamos bien informados acerca de las amenazas en curso o emergentes, quisiera subrayar un incidente notable.

El DNS se creó en 2010 y después de un par de años hubo un evento, en julio de 2012, cuando una plataforma; muy popular de hosting, fue explotada, esto se vio claramente porque pudimos ver más de 100 nombres de dominios .SG, que se usan para phishing, y gracias a nuestro trabajo podemos encontrar al proveedor de hosting

común, entonces rápidamente llamamos al proveedor de hosting y a los diferentes proveedores, y les pedimos a los administradores que retiraran el dominio. Resolvimos este problema de phishing en cuestión de horas.

Otra amenaza emergente que detectamos con el DNS; y esto fue algo muy reciente, fue una biblioteca de código abierto comprometida en 2024, el tema surgió porque un delincuente compró un nombre de dominio, inyectó código malicioso en una biblioteca, entones después de hacer esto se utilizó la biblioteca; como era una biblioteca muy utilizada, esto tuvo un impacto muy amplio y hubo una gran cantidad de dominios afectados. Hicimos lo siguiente. Notificamos a cada registratario para que tomaran las medidas necesarias.

¿Cuáles son los desafíos que vemos nosotros en nuestro trabajo? En primer lugar, para mitigarlos trabajamos en educación y concientización, a pesar de que tenemos un sistema para notificar a los registratarios, a veces los registratarios no sabían qué hacer con la información que les dábamos y a veces cuando buscamos a los proveedores de hosting no conocen el problema y tampoco saben qué hacer con la información que nosotros les dábamos.

En segundo lugar, observamos una demoras en la resolución, creo que, esto se debe a que algunos de los registratarios están tratando de encontrar al proveedor de hosting y algunos de los proveedores de hosting, además, dudan en enfocarse en este problema, en

atacarlo, porque esto puede molestar a alguno de sus otros clientes.

En tercer lugar, buscamos… En un caso determinado quisimos retirar un nombre de dominio, en un caso hubo un delincuente que tenía conocimientos técnicos, notificamos a la víctima, en ese caso, y le enseñamos a dar de baja este dominio que causaba problemas.

¿Cuál es el impacto de todas estas estrategias de mitigación? En primer lugar, mantener bajo los niveles de uso indebido, tuvimos aproximadamente cinco casos confirmados por mes. Logramos crear consciencia entre la comunidad, entonces una vez que nuestro sistema envía una notificación de correo electrónico, o a través de estos correos electrónicos, creamos consciencia entre todos los que fueron recibiendo estos correos electrónicos, además, fueron aprendiendo cómo proteger sus sitios web y a sus nombres de dominios.

Además, logramos mantener la confianza en el .SG, logramos garantizar que .SG siga siendo algo seguro y confiable para la población y las empresas. En tercer y cuarto lugar, hay más confianza en el gobierno, esos esfuerzos para lograr que se confíe en .SG tuvieron muy buenos resultados y al SGNIC se le encargó que operara el SSIR, que desempeña un papel muy importante, estamos hablando de un registro específico de ID de remitentes de SMS.

NICK WENBAN-SMITH

Gracias. Tenemos algunas preguntas, pero antes quisiera escuchar la presentación de Bruce y después vamos a tener bastante tiempo para las preguntas, gracias a los panelistas por abstenerse al tiempo que les asignaron, pero sigan enviando sus preguntas, si están en Zoom mándenlas por aquí y voy a tratar de distribuir en forma equitativa las preguntas que se planteen entre los que están en la sala y los que no lo están. Bruce, le damos la palabra.

BRUCE TONKIN

Muchas gracias, Nick. En esta sesión hay algo que me parece útil y algo que también vimos en otras sesiones, hablamos de phishing y malware, y Gabriel dijo que phishing internacionalmente tiene cifras muy altas, nosotros nos centramos en esto desde hace un par de años y hemos visto una reducción en la cantidad de delitos de phishing en .AU. Lo que nos queda básicamente son los sitios web comprometidos, que han sido usados para hacer phishing, pero no tanto personas que registraron un dominio para hacer phishing.

Lo que estamos viendo ahora es que, formamos parte de un ecosistema mucho más amplio y para darles el contexto de Australia, tenemos una economía prácticamente 100% digital donde en muchísimas semanas yo no uso efectivo, así que, todas las transacciones son electrónicas y en el pasado si se cometía un delito o una estafa en un bar local, esto se podía atacar en forma presencial porque veíamos a la persona que estaba tratando de estafarnos en ese bar, pero en el mundo online esto es más difícil.

Además, muchos de estos fraudes se inician fuera de Australia, entonces ahora es muy difícil encontrar al culpable real, pero lo que tratamos de hacer es interrumpir sus actividades y esperar que vayan a otro lado. El gobierno se centró en un marco de prevención de estafas y aquí se consideran los aspectos financieros, cómo se reciben los pagos, analizamos la parte de telecomunicaciones; son los mensajes SMS que se utilizan y, creo que, Gabriel ya mencionó que esto se utiliza para empezar las estafas.

También trabajamos con empresas de telecomunicaciones y las plataformas digitales, las redes sociales, Facebook, etc., y hay que trabajar en cooperación con todo el ecosistema porque cada parte del ecosistema tiene un rol. Nosotros tenemos un centro anti-estafa nacional financiado por el gobierno y allí se coordinan a nivel nacional las estafas, además, hay otra actividad interesante en nuestro entorno, que son las apuestas, que son muy populares en Australia.

Se están haciendo estafas a través de estas apuestas, especialmente en fútbol, hay muchas estafas aquí, estos son los links que tenemos en pantalla para que puedan acceder a la información relacionada con esas estafas. La próxima diapositiva, por favor.

En Australia tenemos algunas definiciones que, creo que, son muy útiles, una estafa debe involucrar engaños y si tiene resultados positivos debe llevar a pérdidas o daños, y estamos hablando de información en cuanto a cómo se puede actuar, es información que

tiene una empresa y que indica que una actividad está relacionada con su negocio, además, en este ecosistema recibimos información de muchas fuentes y podemos usar esa información para indicar que, quizás, se esté dando un fraude usando un nombre de dominio y después podamos actuar.

Entonces este es el marco que desarrolló el gobierno de Australia y, creo que, es bastante bueno porque básicamente dice: "Estos son los pasos que una organización, que forma parte del ecosistema, debe seguir". En primer lugar, debemos tener procesos proactivos para combatir las estafas, se deben tener pasos razonables para evitar las estafas. Para nosotros la prevención es lo que hacemos al principio, hacemos una verificación inicial de las registraciones, verificamos las registraciones que vienen de los registradores y también verificamos la renovación de registraciones…

Perdón, detectamos, es decir, tomamos medidas razonables para detectar las actividades y, creo que, esta semana ya se mencionó esto en algunos de los debates de políticas en diferentes grupos, pero consideramos, por ejemplo, los nombres, cuando hay muchos nombres que se registran en poco tiempo y quizás esto sea legítimo, pero, por lo menos, hay que tomar medidas para identificar estas cuestiones e investigarlas.

Alterar, es decir, se toman pasos razonables, por ejemplo, si detectamos una estafa; y ya esta semana algunas personas lo dijeron, que generalmente estas actividades se hacen por lotes,

entonces hay una o dos personas tratando de registrar cientos de nombres y vamos viendo cuál es el patrón, y cuando detectamos el patrón podemos eliminar todo ese lote de nombres, después hay que monitorear un par de semanas porque van a seguir intentándolo, van a seguir registrando nombres utilizando el tipo de estafa anterior.

Y si seguimos dándolos de baja impidiendo que los registren van a ir a buscar otro código de país u otro dominio de alto nivel, de los que tenemos aquí, por ejemplo. Por eso nosotros debemos compartir información porque cuando se le impide a un delincuente actuar en una zona, pasa a otra. Obviamente se trata de responder a los informes y es el último punto el que estamos tratando de resolver, ¿cómo informamos lo que estamos viendo? Para que sea información útil para otros de los que están presentes en esta sala.

Quería mencionar los dos tipos de problemas relacionados con los nombres de dominios. Bien, una categoría es la de actividades maliciosas, en este caso, el registratario utiliza información falsa y a pesar de que tenemos pasos de verificación, si se utiliza información robada o un tercer, el pasaporte robado o una identificación robada, bueno, esto se puede detectar no tan fácilmente, pero, creo que, ahora los delincuentes están volviéndose más sofisticados y utilizan información robada para registrar nombres de dominios.

Lo que tenemos a nuestro favor es que tenemos los requerimientos de presencia en Australia, esto se vio también en Singapur, creo que, ya lo mencionaron, porque un nombre de dominio tiene que estar registrado con el país y eso se puede utilizar para detectar la información falsa.

Entonces cuando vemos un nombre que se utiliza para una estafa financiera no retiramos el nombre de dominio por una estafa financiera, sino que, damos de baja el dominio porque se utilizó información falsa. Tomamos información de los organismos de aplicación de la ley, no hace falta que nos manden necesariamente un mandamiento judicial, nos dicen: "Creemos que este sitio es maliciosos", y después simplemente lo damos de baja nosotros, si se utilizó información falsa para crearlo, no hace falta esperar un mandamiento judicial, lo damos de baja por información falsa.

Otra categoría son sitios comprometidos, hay algunas soluciones ya definidas, listas para preparar, listas para utilizar, que se pueden emplear directamente para dar de baja e identificar estos sitios web comprometidos, los sitios web son hackeados, a veces se utiliza una versión sin los parches para hacer estas estafas. En general, no damos de baja el nombre de dominio porque la empresa dejaría de operar, simplemente podemos encontrar todo con el registrador y el registratario, en general, los registratarios se sorprenden mucho porque se enteran que están dando el hosting a un contenido negativo o malicioso y actúan de manera muy proactiva.

También hay un tema de educación al usuario porque cuando nos ponemos en contacto con el registratario ni siquiera sabe, a veces, quién es el hosting, la persona que creó el sitio web ya dejó la empresa, entonces lleva un cierto tiempo corregir todo esto y les ayudamos nosotros. Es importante entender el ecosistema, saber con quién hay que hablar y con quién hay que comunicarse para resolver el problema que tiene el sitio web o retirarlo.

Aquí utilizamos el mismo marco, el marco antifraude de Australia a nivel de gobernanza, hacemos un seguimiento de todos los informes y nuestras investigaciones se la informamos a la Junta Directiva, tenemos un proceso de validación, esto es un acto de prevención, detectamos, es decir, después de que se registró un nombre lo verificamos y buscamos patrones asociados con las estafas. Por ejemplo, hacemos búsquedas en Google para ver el contenido y encontramos los dominios que siguen este patrón, buscamos diferentes marcadores en los datos de registración y retiramos grandes lotes de nombres.

Y también alteramos, buscamos proactivamente los dominios relacionados, si hay un dominio que ha sido utilizado para un fraude seguramente haya otros dominios muy parecidos que también sean utilizado para lo mismo. Tratamos de responder y trabajar con los organismos de seguridad y los invitamos a que nos traigan la información, pero afuera, además de la información que recibimos de las autoridades de aplicación de la ley, es muy poca esa información, así que, en general, tratamos de obtener información de otras fuentes, inteligencias sobre amenazas, etc.,

pero también trabajamos con las autoridades de aplicación de la ley, como dije.

El último punto; y esto es alentador, tenemos que pensar en esto como comunidad, ¿cómo compartimos información? Es difícil porque no hay que compartir información que viole las leyes de privacidad, pero cuanto más información compartamos o cuando detectamos algo que sea inusual seguramente también lo mismo esté sucediendo en otros ccTLD o gTLD, por eso tenemos que trabajar con alguien como la IIF, que mencionó Keith, y con otros actores del ecosistema.

Se trata no solamente de actuar contra un dominio malicioso, sino contra todos los demás delincuentes que estén trabajando en este espacio.

NICK WENBAN-SMITH Muchas gracias, es mucha información que recibimos ante el hecho de que esto está a una escala muy grande y estamos aquí defendiendo los intereses de los ciudadanos, y también tomar en cuenta el impacto que esto tiene en las operaciones de registros donde se requiere tiempo y esfuerzo, pero realmente esto aún así es una fracción muy pequeña compararlo con las pérdidas y los daños que reciben los consumidores.

También es un problema la confiabilidad y la reputación, a medida que aumenta la digitalización, que las personas tengan confianza, que sepan con quiénes están lidiando en cuanto a estos servicios.

Yo sé que tenemos algunas preguntas y, creo que, Olga fue la primera, tenemos como 15 minutos, creo, así que, le doy la palabra a Olga y los demás pueden alzar sus manos tanto en la sala como virtual en Zoom.

OLGA CAVALLI Gracias por sus presentaciones. Tengo una pregunta para el representante del FBI, perdone que se me olvidó su nombre, en cuanto a la cantidad de pérdidas o daños, que usted mencionó en su presentación, ¿recibió la información de las víctimas o tiene usted un método para poder calcular el daño? En base al daño recibido de parte de las víctimas, ¿puede explicar eso?

GABRIEL ANDREWS Gracias por la pregunta. Muchas de las cifras con respecto a daños son autoreportados, a medida que progresa el caso y pasamos a un nivel de denuncia, de procesar cargos en contra del delincuente, entonces podemos validarlas, pero cuando estamos recuperando o colectando, o reuniendo, estadísticas es información que proporciona la víctima.

Hay, a veces, víctimas que exageran los daños, por ejemplo, amenazas o daños en su marca o imagen, eso no lo incluimos, pero, por ejemplo, tuvimos un caso de un ataque de Ransomware y nos obligaron a pagar $5 millones para tener acceso a la red, de nuevo, eso obviamente es un gran daño. O tuvimos una transferencia inalámbrica donde una víctima le pagó a un vendedor y lo hizo a

través de un correo electrónico comprometido, entonces de ahí es donde sacamos las cifras.

NICK WENBAN-SMITH Vamos con la pregunta de Hilde.

HILDE THUNEM Soy Hilde Thunem del registro de Noruega. Tengo dos preguntas, la primera es para el FBI, investigación reciente que he visto parece indicar que 80% del phishing surge de dominios comprometidos, 20% viene de las registraciones maliciosas con la excepción de que, cuando hay un requisito de presencia local, disminuyen las registraciones maliciosos. Entonces me pregunto, cuando ustedes lidian con un caso y ven un patrón, supongo, ¿hay una diferencia en cómo tratan este dominio comprometido? Porque de pronto la persona tras el dominio es una víctima y me imagino que ustedes no se comunican con el registro, y piden que desactiven o remuevan el nombre de dominio, espero que no.

GABRIEL ANDREWS Bueno, es una pregunta importante y tiene razón, en respuesta a los hechos y las circunstancias que usted tiene, pues en cualquier momento dado cambiaría y uno tiene que pensar cuál es la respuesta responsable ante el cambio. Cuando uno escucha de un delito, o algo que se denuncia, hay que, primero, pensar es en dónde el maleante está controlando la infraestructura o es un cliente de un negocio legítimo, por ejemplo, si están utilizando un

sitio web y está comprometida una persona toma tiempo investigar eso, pero cuando estamos mitigando el daño usted tiene razón, sería más razonable si se pudiera identificar el dominio que ha sido registrado maliciosamente, en vez de hacerle la pregunta a un registrador u operador de registros a que lo remueva.

Eso se haría como primera opción cuando hay un sitio comprometido, pero de pronto eso agrega una víctima más que tendría que incluirse cuando se procesan cargos penales, si los Estados Unidos consiguiera acceso no autorizado de ese tipo es en contra la ley también, entonces hay que mantener un equilibrio.

HILDE THUNEM

Me gustaría saber qué están pensando en cómo lidiar con lo comprometido, que es una gran cantidad de esas estafas, pero ¿cuál es su experiencia? Cuando se trata de comunicar con una persona y les dice que su sitio web está comprometido porque yo sé que como registro uno es invisible, pero, a veces, si uno se comunica con la persona para decirle que hay una estafa, ellos podrían ver eso mismo como una estafa, entonces definitivamente prefiero que no sea yo, sino la policía o alguna autoridad haga eso y especialmente cuando se quiere que se haga algo con un sitio web habría que hacerlo rápidamente para evitar más estafa.

GABRIEL ANDREWS

Todos estamos con la cabeza acertando que estamos de acuerdo, tiene razón, hay retos en tener que notificarles a las víctimas y en

el pasado al colaborar con sectores privados en grandes remociones de este tipo hay que colaborar, a veces, con compañías grandes tecnológicas o compañías de infraestructura de internet, como Microsoft, hay que mantener un equilibrio en cuanto a hasta qué punto uno va a confiar en el sector privado para hacer esto, o no.

En el pasado nosotros pensábamos que era razonable que los ISP le notificaran a los clientes, creo que, esto pasó en casos del DNS en lo que tiene que ver con lo que llaman envenenamiento del caché, pero lo que ocurrió es que los clientes del ISP se enojaron con los proveedores de servicios de internet porque empezaron a echarles a ellos la culpa con respecto a las cosas comprometidas, cuando no tenían nada que ver con eso, sino que, estaban tomando una acción responsable.

Los organismos de cumplimiento de la ley reconocen eso y ellos tienen un rol en ayudar a las personas y a las víctimas, pero hablando de mi mismo, yo lo veo como mi rol el hacer esto y ayudar a las personas, pero reconozco que es un reto y no fácilmente se puede resolver, desafortunadamente.

NICK WENBAN-SMITH

Pierre y después Brian Cimbolic, o Hilde. ¿Ustedes apoyarían al que registró? Como soy abogado, hago la pregunta, ¿estarían de acuerdo en que ellos introduzcan requisitos legales a los

registratarios para que ellos mantengan una higiene básica de seguridad en sus sitios web?

HILDE THUNEM: No, porque no requiere que ellos tengan un sitio web, sino que, están comprando un nombre de dominio y el derecho a usarlo, y el derecho a que pongan algo para una dirección IP, no es necesario tener un correo electrónico ni un sitio web, esos son opciones que ellos mismos tienen que comprar.

Y según la ley de comunicación electrónica en Noruega, yo no soy responsable en cuanto al uso del nombre del dominio, cuando pongo algo que no estoy obligada a entregar no lo puedo hacer, según el contrato, más bien hay que verlo de dos vías y se espera que ellos no hagan algo que no deben hacer, pero yo no lo apoyaría en un contrato, de que se diga eso.

NICK WENBAN-SMITH: Pierre.

PIERRE: Gracias, Nick y gracias por esta sesión interesante y diversa. Primero, quiero decir que, como siempre, estoy de acuerdo con esta respuesta de no, no estaría de acuerdo con lo que dijo Hilde, ahora, esto no quiere decir que nosotros no tengamos que reaccionar cuando vemos un problema en el sitio web. Es diferente si uno pone en el contrato algo como, por ejemplo, “hay que asegurarse de mantener la seguridad del sitio web”, pero la

pregunta que haría después es, ¿cómo puedo yo hacer cumplir mis propios contratos? ¿O cómo verifico yo que el registratario ha cumplido con esto en su sitio web?

No estoy a favor de poner algo en el contrato que yo mismo no puedo hacer cumplir, pero la pregunta que yo tengo para los panelistas, especialmente quien representa al FBI, si se pudiera compartir información con respecto al tipo de conversación que tiene con estas compañías telefónicas, ¿podría hablar de eso? Porque estamos hablando acerca de los datos en el WHOIS, la mayor parte de las estafas, por lo menos en Francia, lo recibo de mensajes de texto en mi IPhone y no son números ocultos, son números reales.

Y yo supongo que las personas que me están mandando este tipo de cosas no dieron su nombre y dirección real al operador del teléfono porque si no sería muy fácil poder agarrarlos, ¿no? No sé cómo funciona esto, pero estoy viendo más que a bancos y a los ISP se les pide que hagan la verificación y hacerlo en el mundo Telecom, a veces, eso tampoco funciona.

Entonces yo quiero saber, ¿cómo lidia usted con eso? Gracias.

GABRIEL ANDREWS

Reconozco que es una pregunta válida, justa y disculpo que no tengo una buena respuesta para usted porque últimamente, según mi memoria, no he hablado con operadores telefónicos, pero diría que a través de todo el espectro hay un reconocimiento

aumentante que en la sociedad van a existir retos con respecto a la autentificación de identidad.

Y aún con herramientas como la IA ellos han tenido mucho éxito en usurpar la identidad de una persona y cuando estamos hablando de retos, de lo que ocurre en línea, nos preguntamos, ¿cómo podemos confiar ya en esto? Hay mucho más que decir en el tema, simplemente no pienso que soy la persona adecuada para decirlo.

PIERRE

Yo entiendo que usted no esté preparado para contestar eso, pero es justo decirte que los números de teléfonos son identificadores, nadie toma el error de pensar que los números de teléfonos son contenidos, nombres de dominios son identificadores, así que, hay un verdadero vínculo entre esas dos cosas. Creo que, realmente debemos entender bien, pero como lo hace la industria telefónica porque siempre estamos hablando de los identificadores y no el contenido. Gracias.

NICK WENBAN-SMITH

Bruce y después Keith.

BRUCE TONKIN

Es exactamente lo que está tratando de hacer el gobierno australiano, cada grupo dice que es problema del otro, pero hay que combinarlo porque normalmente es algún tipo de mensaje de SMS, por ejemplo, hay un banco a donde va el dinero y después hay un nombre de dominio donde hay un enlace con el mensaje de

SMS, es una combinación. En Australia, aunque es por teléfono, uno puede reportarlo como una estafa porque cuando uno lo va a borrar, pregunta: “Lo va a borrar solamente o lo va a borrar porque es una estafa”.

Eso es lo que se trata de hacer en Australia porque es una manera de conectar los puntos para llegar al maleante, entonces el problema son los números de celulares que lo causa y después no hay un enrutamiento de uno al otro.

KEITH DRAZEK: En el foro de infraestructura de internet nuestra visión, a medida que esto evoluciona, es incluir los telcos o lado telefónico, incluir estos procesadores de pago cuando estamos hablando de fraude financiero, entonces, creo que, la expectativa es que, a medida que tenemos registros, registradores web y demás, se continúa agregando jugadores adicionales con diferentes roles que pueden mitigar estos daños, todos tenemos diferentes áreas de responsabilidad y capacidades técnicas, pero lo importante es la coordinación y esa es una de las metas de estos esfuerzos. Gracias.

NICK WENBAN-SMITH: Gracias. Ahora le doy la palabra a Brian.

BRIAN CIMBOLIC: Hola, soy Brian Cimbolic del registro de interés público. Gabriel, esta es una breve pregunta para usted con respecto al informe de delitos de internet en línea, ¿eso es puramente para delitos

relacionados con nombres de dominios o también incluyen plataformas de redes sociales?

GABRIEL ANDREWS Es para cualquier delito relacionado con el internet, hay muchas categorías y por eso lucho para que sea algo relevante, cuando menciono que se traslapan, pero no, se trata de un área general.

BRIAN CIMBOLIC ¿Tenía usted alguna idea de cuáles eran de las redes sociales y cuáles eran de nombres de dominios?

GABRIEL ANDREWS Sí, pero no es algo tan fiel, lo están dividiendo en grupos más grandes con phishing, pero no sé si ahí lo dividen si es phishing o es comparado con WhatsApp, aplicaciones de chat, dominios… O sea, su pregunta es relevante, pero no tenemos esos datos detallados.

BRIAN CIMBOLIC Sería bueno tener ese tipo de desglose porque eso ayuda a saber qué es lo que está ocurriendo en las plataformas de redes sociales versus el DNS.

GABRIEL ANDREWS Sí, sería bueno tener un informe fiel en cuanto a eso, pero trabajaremos en eso con el tiempo.

NICK WENBAN-SMITH

Ese es un tema fascinante y por eso es importante tener estas sesiones para poder hablar de este tema a través de diferentes actores y ver las diferentes perspectivas porque el entender el contexto de algunas de estas cifras, que se han presentado, creo que, es importante como operadores técnicos en esta infraestructura, que hagamos lo suficiente para impedir estos tipos de delitos, pero tal vez entender donde en otros lugares, que no se destacan tanto, se puedan incluir y también hablar con nuestros amigos del gobierno y reguladores de políticas para ayudar a solucionar esto.

Vamos a tomar, otra vez, una votación y vamos a ver la pregunta. Bueno, se está contestando la pregunta, la pregunta es, "¿en qué nivel está usted de acuerdo con la siguiente declaración?" Extremo izquierdo es que está muy en desacuerdo, extremo derecho es que está muy de acuerdo.

La declaración es la siguiente. Nuestro registro está bien preparado para detectar uso indebido del dominio vinculado con delitos financieros. La otra es: Nuestro registro está bien preparado para responder al uso indebido de dominios vinculado con delitos financieros. Hay algunas personas que piensan que los registros todavía no están bien preparados para detectar el uso indebido, el tema es que hay mucha complejidad relacionada con los sitios web comprometidos.

Y, finalmente, quería aplaudir a los miembros del panel, muchísimas gracias. Las diapositivas incluyen algunos de los recursos que se pueden utilizar desde DASC y otra información relevante para esta sesión es que, eso está en las diapositivas, pueden verlo después. Y dicho esto, muchísimas gracias y vayamos a disfrutar de la pausa del café.

[FIN DE LA TRANSCRIPCIÓN]