Boletín de Fraude 15 de Junio 2021.

01 **Estima UIF fraudes de Florian Tudor en 240 millones de dólares.**

02 **‘Rey del fraude’ ruso es detenido por estafa millonaria con granja de bots.**

03 **Reconoce Banxico 16 hackeos a bancos.**

.

04 **Brasil investiga a la petrolera estadounidense Freepoint por supuesta trama de sobornos.**

05 **Peugeot será procesado en Francia por caso de dieselgate.**

06 **Más de 1,000 detenidos en China por fraudes relacionados con criptomonedas.**

¿HAS SIDO VÍCTIMA DE FRAUDE O AÚN NO LO SABES?

CONTÁCTANOS

protiviti®

Face the Future with Confidence

Protiviti líder en servicios de consultoría de riesgos de negocios y auditoría interna, apoya a la lucha antifraude.
Quincenalmente distribuimos esta recopilación de las notas más sobresalientes relacionadas con delitos de cuello blanco.

protiviti®
Face the Future with Confidence

Estima UIF fraudes de Florian Tudor en 240 millones de dólares.

01 junio 2021

El Economista.

La Fiscalía General de la República (FGR) confirmó la detención en Quintana Roo de Florian Tudor, presunto líder de la Banda de la Riviera Maya.

Santiago Nieto, titular de la Unidad de Inteligencia Financiera de Hacienda (UIF) declaró que la organización delictiva del detenido tenía ganancias cercanas a los 240 millones de dólares anuales por la presunta clonación de tarjetas bancarias en zonas turísticas del país.

A raíz de las investigaciones contra esta organización, Nieto Castillo declaró que la UIF logró congelarle hasta 520 millones de pesos en el sistema financiero e incluso los señalados lograron interponer recursos para su descongelamiento.

“Esta banda de rumanos ganaba 240 millones de dólares anuales a partir de la clonación de tarjetas y hoy se detuvo a esta persona (Tudor)... Llegamos a bloquear 520 millones de pesos de este grupo, ellos están promoviendo una serie de juicios de amparo e inclusive el señor Tudor buscó una garantía de audiencia ante la UIF, pero nunca compareció, por tanto sus cuentas permanecen bloqueadas”, declaró Nieto Castillo.

De acuerdo con el funcionario, la investigación realizada tanto a Tudor como a su organización arrojó que se tenía relación con más de 20 empresas, que presuntamente fueron utilizadas para el blanqueo de capitales.

Florian Tudor fue detenido en cumplimiento de una solicitud de detención con fines de extradición, formulada por el Gobierno de Rumania, por delitos de delincuencia organizada, extorsión y tentativa de homicidio agravado.

La orden de aprehensión fue tramitada y obtenida por la FGR ante un juez de Control del Reclusorio Norte.

La FGR precisó que durante la diligencia de aprehensión, un agente del Ministerio Público Federal intentó obstaculizar la acción, mientras que el abogado del empresario rumano agredió a golpes a los agentes de la Policía Federal Ministerial.

Ambas personas también fueron sometidas y detenidas para ponerlas a disposición del Ministerio Público Federal, por los delitos que correspondan.

El rumano llegó a México en el 2011, luego de ser liberado en Roma por introducir un chip a un cajero automático.

Según las investigaciones federales, el hoy detenido creó en Quintana Roo una red de clonadores de tarjetas mediante skimmers, tecnología que es introducida a los cajeros automáticos para leer la banda magnética de las tarjetas bancarias, e identificar el NIP.

Las autoridades presumen que Tudor se habría aliado a Leticia Rodríguez Lara, alias Doña Lety, quien fue detenida en el 2017 por ser presunta operadora del Cártel de Cancún.

Ejército Nacional 843 – B Piso 5, Colonia Granada Ciudad de México, Alcaldía Miguel Hidalgo Conmutador 6729- 8070 Fax: 5511.2500

Conoce más sobre Protiviti

Para recibir o anular tu inscripción, envía un correo a servicio@protivitiglobal.com.mx con la palabra “ALTA” o “BAJA” en el asunto™

protiviti®
Face the Future with Confidence

‘Rey del fraude’ ruso es detenido por estafa millonaria con granja de bots.

Un ciudadano ruso fue declarado culpable de los cargos estadounidenses de utilizar una granja de bots y alquilar servidores para falsificar el tráfico de internet en los sitios de medios, lo que provocó que otras empresas pagaran tarifas publicitarias infladas.

02 Junio 2021

El Financiero.

Aleksandr Zhukov, de 41 años, fue el autor intelectual de un esquema conocido como Methbot en el que se emplearon mil 900 servidores para crear millones de visualizaciones de anuncios falsos en línea en sitios web, incluidos los del New York Times y el Wall Street Journal, dijeron los fiscales. Zhukov ganó 7 millones de dólares con el negocio y canalizó el dinero a bancos de todo el mundo, según Estados Unidos, que citó un texto en el que se describía a sí mismo como el “rey del fraude”.

Los miembros del jurado de la corte federal en Brooklyn, Nueva York, emitieron el veredicto el viernes.

A empresas como PepsiCo, organizaciones benéficas y otros anunciantes se les cobraron tarifas infladas solo para que los robots digitales “vieran” sus anuncios, dijo Estados Unidos. En efecto, Zhukov y sus coconspiradores en Rusia y Kazajstán corrompieron el complejo y vulnerable ecosistema de la publicidad en línea al usar servidores alquilados en Dallas y Ámsterdam para eludir las protecciones contra el fraude y simular la actividad en línea de millones de personas que ven anuncios en línea, dijeron los fiscales.

Zhukov subió al estrado durante el juicio de tres semanas, alegando que nunca engañó a nadie y pensó que solo le estaba dando a la industria lo que quería: una forma de aumentar de manera económica, aunque artificial, el tráfico del sitio.

“No había nada que ocultar”, testificó. “¿Por qué mentirles si tenemos tráfico de bots? ¿Por qué mentir, tratar de venderlo como humano si es un robot? Estábamos haciendo negocios. No estamos cometiendo estafas ni fraudes”.

Zhukov fue arrestado en Bulgaria en 2018 y extraditado a Nueva York. Fue acusado de conspiración de fraude electrónico, fraude electrónico, conspiración de lavado de dinero y participación en transacciones monetarias que involucren bienes derivados de actividades ilegales.

protiviti®
Face the Future with Confidence

Reconoce Banxico 16 hackeos a bancos.

Instituciones del sector financiero en México registraron 16 ataques cibernéticos de 2019 a enero del presente año, los cuales tuvieron un costo de 785.4 millones de pesos, de acuerdo con reportes del Banco de México (Banxico).

04 junio 2021

El Financiero.

Según los registros del banco central sobre los "Principales incidentes cibernéticos ocurridos en el sistema financiero nacional", fue en 2019 cuando se registraron las mayores afectaciones, superando incluso al 2020 cuando se incrementó el uso de banca por Internet y móvil derivado de la pandemia.

Si bien el nombre de los afectados no es público, Banxico sí comparte detalles sobre estos ciberataques; en sus registros detalla cómo fue, si hubo afectaciones a clientes y lo más importante, para medir el impacto económico, y es un dato que ningún banco comparte públicamente, es a cuánto ascendió el monto de esos ataques.

En los incidentes destaca el hecho de que se reconoce por primera vez, que, en 2019, el banco central registró 8 ataques por un monto total 784.7 millones de pesos, que implica el monto más alto registrado hasta la fecha.

En los datos se confirma que en septiembre de 2019 un banco tuvo un ataque que les permitió a los ciberdelincuentes sustraer dinero, después de iniciar una sesión en un dispositivo móvil con claves robadas a los cuentahabientes.

Los atacantes lograron vulnerar los controles de la aplicación del banco para enviar transferencias por montos superiores a los permitidos, aprovechando deficiencias en los procesos de validación y control.

En ese mismo mes, un ataque a otro banco se concretó, según se explica en el informe, después de iniciar una sesión en un dispositivo móvil, también con claves robadas a los clientes; los atacantes lograron vulnerar los controles de la aplicación del banco para enviar transferencias a cuentas no pre-registradas por el cliente, aprovechando deficiencias en los procesos de validación y control del sistema. Ambos tipos de ataques no han sido reconocidos por ningún banco.

En ese año, fue en mayo el mayor fraude cibernético, el cual fue ejecutado por personal de terceros que laboraba al interior de un banco de inversión, quienes mediante la inyección de operaciones apócrifas de depósito de intereses a cuentas de cheques lograron sustraer 462 millones de pesos en tres días.

Bajan ataques en 2020

En 2020, Banxico registró únicamente 5 ataques, en donde no hay un monto aún reportado de afectación, pero si muestra que fueron afectados en abril por un ransomware en servidores de un banco comercial, en donde la banca por Internet fue la perjudicada.

protiviti®
Face the Future with Confidence

Reconoce Banxico 16 hackeos a bancos. (Continuación

04 junio 2021

El Financiero.

En mayo de ese año otro banco fue atacado, afectando los equipos de cómputo de sucursales, ahí los servicios en ventanilla quedaron sin servicio.

En noviembre se tuvo registro de otros dos ataques, uno a una casa de bolsa que también fue perjudicada y no pudieron realizar dispersión de fondos, y el otro fue a una casa de bolsa perteneciente a un grupo financiero, ellos en ese mes no pudieron dar el servicio de banca por Internet, ni de operaciones cambiarias y dispersión de fondos.

Pese a existir grupos de trabajo de ciberseguridad en el sector financiero para compartir información de los ataques que han recibido y alertar a sus colegas, se utilizaron los mismos virus; así los diferentes tipos de ransomware identificados en los incidentes fueron: MedusaLocker, Sodinokibi, Crysis/Phobos y Emotet.

En enero de este año, Banxico tiene oficialmente registrados tres ataques cibernéticos, dos a cajeros automáticos de dos instituciones de crédito y a un tercero, afectado en su banca en línea; en los tres ataques se utilizó un ransomware identificado en el incidente como REvil, también conocido como Sodinokibi.

La afectación según el reporte fue en un caso por 570 mil pesos, a otro por 130 mil pesos y el tercer ataque que afectó la banca por Internet de otra institución no se reveló, en los tres casos se asegura que los clientes no fueron afectados.

protiviti®
Face the Future with Confidence

Brasil investiga a la petrolera estadounidense Freepoint por supuesta trama de sobornos.

Autoridades de Brasil están investigando a funcionarios de alto rango de la empresa Freepoint Commodities, con sede en Connecticut, por su presunto papel en un esquema de sobornos que involucra a la compañía petrolera estatal Petrobras, según pudo comprobar Reuters.

04 junio 2021

El Economista.

La policía federal brasileña sospecha que Freepoint envió sobornos a empleados de Petrobras a través de un intermediario durante un período de aproximadamente siete años que terminó en 2018. Reuters reconstruyó la supuesta operación a partir de tres personas cercanas a la investigación, que hablaron bajo condición de anonimato, y de cientos de páginas de documentos judiciales presentados por los investigadores brasileños que no fueron divulgados anteriormente.

Según las fuentes y los documentos judiciales revisados por Reuters, que la policía brasileña presentó el año pasado a un juez federal que supervisa la investigación, se sospecha que al menos dos empleados de alto rango de Freepoint, incluido Robert Peck, jefe del negocio petrolero global de la empresa, participaron en la supuesta trama.

Esos documentos incluyen registros bancarios, facturas, correos electrónicos y mensajes de WhatsApp intercambiados entre los presuntos involucrados, incluyendo a Peck. La investigación brasileña no fue informada previamente. No se han presentado cargos y no está claro si se presentarán. Las autoridades están investigando a la propia Freepoint, lo que podría dar lugar a posibles multas u otras sanciones civiles, si se descubre que la empresa cometió alguna infracción.

En respuesta a preguntas de Reuters sobre la investigación en Brasil, un portavoz de Freepoint dijo en un correo electrónico que la empresa "está firmemente comprometida con el cumplimiento de las leyes en todos los lugares en los que hacemos negocios" y declinó hacer más comentarios. Freepoint denegó los pedidos para que Peck esté disponible para una entrevista. Peck no contestó las preguntas que Reuters le envió a través de LinkedIn. Una mujer que respondió al teléfono en su casa se negó a hacer comentarios.

Petrobras dijo en un correo electrónico que tiene "tolerancia cero en relación con el fraude y la corrupción", y que los empleados involucrados en irregularidades en su unidad de comercio "fueron inmediatamente despedidos por causa justificada en 2018". La policía federal de Brasil no respondió a las solicitudes de comentarios y el Departamento de Justicia de Estados Unidos declinó comentar si está investigando el asunto de Freepoint.

La investigación de Freepoint se produce en el marco de una ofensiva más amplia de las fuerzas de seguridad contra las empresas de comercio de materias primas implicadas en presunta corrupción, en especial en América Latina.

Freepoint es el primer operador energético importante estadounidense que ha sido objeto de una investigación reciente en Brasil. La empresa, con sede en Stamford, compra y vende todo tipo de combustible a través de operaciones en tres continentes y emplea a más de 500 personas en todo el mundo.

protiviti®
Face the Future with Confidence

Brasil investiga a la petrolera estadounidense Freepoint por supuesta trama de sobornos. (Continuación)

04 junio 2021

El Economista.

El supuesto esquema

La investigación de Freepoint forma parte de una más amplia de las autoridades brasileñas conocida como "Lava Jato", que terminó oficialmente en febrero. Algunas investigaciones restantes en etapas avanzadas, incluyendo la de Freepoint, han continuado.

En el centro de la investigación de Freepoint se encuentra un exempleado de Petrobras llamado Rodrigo Berkowitz, que anteriormente trabajó como vendedor de combustible para el gigante petrolero brasileño en Houston.

En febrero de 2019, Berkowitz aceptó declararse culpable de cargos en Estados Unidos de conspiración para cometer lavado de dinero, por aceptar sobornos de empresas de comercio de combustible que hacían negocios con Petrobras.

Berkowitz, que sigue viviendo en Houston, está a la espera de la sentencia y colaborando con las autoridades estadounidenses y brasileñas en las investigaciones en curso sobre la industria del comercio de materias primas, según su abogado Jorge Camara, quien declinó hacer más comentarios.

Berkowitz describió el presunto esquema de sobornos de Freepoint en presencia de investigadores estadounidenses y brasileños en diciembre de 2019, según los archivos judiciales que resumen su testimonio.

Petrobras, el séptimo productor mundial de petróleo, subasta habitualmente grandes cargamentos de diversos combustibles para asegurarse de obtener el mejor precio posible por sus productos. Según el testimonio de Berkowitz, él informó a Freepoint sobre las cantidades que los competidores ofrecían en esas subastas. Ese conocimiento permitió a Freepoint aventajar a la competencia, dijo Berkowitz.

A cambio de esa información, según el testimonio de Berkowitz y las facturas obtenidas por la policía brasileña y vistas por Reuters, el vendedor de combustible recibió sobornos de Freepoint a través de un intermediario, un empresario llamado Eduardo Innecco.

Innecco realizó trabajos de consultoría para Freepoint desde aproximadamente 2012 hasta finales de 2018, cuando abandonó abruptamente Sudamérica ante la preocupación de que los investigadores se acercaran, alega la policía brasileña en los archivos judiciales revisados por Reuters.

A través de un representante, Innecco declinó hacer comentarios. "No ha sido acusado de ningún delito y reside actualmente en el sur de Europa", dijo el representante.

Freepoint supuestamente compensaba a Innecco con comisiones que estaban infladas para cubrir el coste de los sobornos, según el testimonio de Berkowitz, los registros bancarios obtenidos por la policía y vistos por Reuters, y las personas familiarizadas con la investigación.

protiviti®
Face the Future with Confidence

Brasil investiga a la petrolera estadounidense Freepoint por supuesta trama de sobornos. (Continuación)

Innecco, a su vez, pasó esos sobornos a los empleados de Petrobras, incluido Berkowitz, según los documentos. Freepoint canalizó casi 500,000 dólares en sobornos a través de Innecco solo entre agosto de 2017 y noviembre de 2018, dijo Berkowitz en su testimonio.

04 junio 2021

El Economista.

La caída

Los implicados en la presunta estafa de Freepoint eran conscientes de los riesgos que corrían a medida que se ampliaba la red del Lava Jato, alega la policía.

El 1 de septiembre de 2018, Innecco envió un mensaje de WhatsApp a Berkowitz, sugiriéndole que transfiera su riqueza al extranjero para protegerla de las autoridades en el caso de que su esquema fuera descubierto, según el testimonio de Berkowitz y una copia del mensaje revisado por Reuters.

Tres meses después, el 5 de diciembre de 2018, las autoridades brasileñas emitieron una orden de arresto contra Berkowitz por aceptar sobornos de empresas de comercio de materias primas.

El 6 de diciembre de 2018, Innecco voló desde su casa en Uruguay a Madrid, según los registros de viaje obtenidos por la policía brasileña y vistos por Reuters. Los investigadores brasileños creen que huyó por temor a que su arresto fuera inminente y las autoridades lo consideran ahora un fugitivo, según los archivos

BOLETÍN DE FRAUDE.

protiviti®
Face the Future with Confidence

Peugeot será procesado en Francia por caso de dieselgate.

Peugeot será imputado en Francia, después de Renault y Volkswagen, como parte de la investigación sobre el fraude en los controles de contaminación de los antiguos modelos de motores diésel, anunció el miércoles Stellantis, casa matriz del fabricante francés de automóviles.

09 junio 2021

El Economista.

Los magistrados de instrucción imputaron este miércoles a Automobiles Peugeot SA, una filial propiedad al 100% de Stellantis NV, "por acusaciones de fraude sobre la venta de vehículos diésel Euro 5 que tuvo lugar en Francia entre 2009 y 2015", explicó el grupo en un comunicado.

Una fuente judicial confirmó el miércoles la imputación de Peugeot por el cargo de "fraude que conlleva un peligro para la salud del ser humano o del animal".

"Otras dos filiales de Stellantis, Automobiles Citroën SA y FCA Italy SpA., serán convocadas por los jueces de instrucción, respectivamente el 10 de junio y en julio, en el marco de la misma información judicial", indicó el grupo.

Peugeot se vio obligado a pagar una "fianza" por valor de 10 millones de euros (12 millones de dólares), incluidos 8 millones de euros (9 millones de dólares) por el posible pago de indemnizaciones y multas, y a presentar una garantía bancaria de 30 millones de euros (36 millones de dólares) "para indemnizar los posibles perjuicios", detalló la empresa.

Peugeot está "evaluando la regularidad de esta medida y si la impugna", advirtió Stellantis en su comunicado.

"Nuestras filiales están firmemente convencidas de que sus sistemas de control de emisiones cumplían todos los requisitos aplicables en ese momento y los siguen respetando hoy en día, y esperan con impaciencia la ocasión de demostrarlo", añade el grupo.

Más de 1,000 detenidos en China por fraudes relacionados con criptomonedas.

12 Junio 2021

El Economista.

Más de 1,000 personas fueron detenidas en China en una operación contra una red acusada de "actividades fraudulentas" relacionadas con criptomonedas, en el punto de mira del gobierno comunista, anunció el ministerio de Seguridad Pública.

China había sido un bastión del bitcóin, la más extendida de las monedas virtuales. Pero Pekín dio un giro radical en 2019 y prohibió los pagos en criptodivisas, acusadas de ser instrumentos al servicio de "actividades criminales."

Las 1,100 personas detenidas el miércoles en todo el país son sospechosas de formar parte de una "organización criminal", según el ministerio de Seguridad Pública.

Se les acusa de utilizar criptomonedas para "blanquear dinero" procedente de estafas por teléfono e internet.

Las detenciones tuvieron lugar en Pekín, la región vecina de Hebei, la región de Shanxi (norte) y Liaoning, una provincia fronteriza con Corea del Norte.

Las autoridades no especificaron las cantidades implicadas ni las criptomonedas utilizadas.

El gobierno está preocupado por el riesgo especulativo que suponen las criptomonedas —anónimas e imposibles de rastrear— para su sistema financiero, así como para la estabilidad social. Sin embargo, se tolera la tenencia de moneda virtual.

En las últimas semanas, China endureció las restricciones a la llamada minería de bitcoines, el proceso de creación de criptomonedas que consume mucha energía.