Instituto Mexicano de Contadores Públicos

En congruencia con los objetivos estratégicos del IMCP, la COMISIÓN DE PREVENCIÓN DE LAVADO DE DINERO Y ANTICORRUPCIÓN prepara este boletín informativo con la finalidad de mantenerlos actualizados en materia de Prevención de Lavado de Dinero y Anticorrupción.

Directorio

Nota aclaratoria

Boletín de la Comisión de Prevención de Lavado de Dinero y Anticorrupción

CONTRARRESTAR EL *RANSOMWARE*

INFORME DEL GAFI DEL 14 DE MARZO DE 2023

C.P. y PCLD Genaro Eliseo Gómez Muñoz
Integrante de la Comisión Nacional de Prevención de Lavado de Dinero y Anticorrupción del IMCP

Los ataques de *ransomware* se dirigen a individuos, empresas y agencias gubernamentales de todo el mundo.

El impacto de estos ataques puede ser devastador para las personas, las agencias gubernamentales y la actividad comercial e, incluso, interrumpir la infraestructura y los servicios esenciales.

Con la publicación del informe de GAFI el organismo analiza los métodos que utilizan los delincuentes para llevar a cabo sus ataques de *ransomware* y cómo se realizan y blanquean los pagos. Los delincuentes utilizan casi exclusivamente criptografía o activos virtuales y tienen fácil acceso a proveedores de servicios de activos virtuales en todo el mundo. Por lo tanto, las jurisdicciones con controles ALD/CFT débiles o inexistentes son motivo de preocupación.

El informe propone una serie de acciones que los países pueden tomar para interrumpir de manera más efectiva el lavado de dinero relacionado con *ransomware*. Esto incluye desarrollar y aprovechar los mecanismos de cooperación internacional existentes, dada la naturaleza transnacional de los ataques de ransomware y el lavado relacionado. Las autoridades también deben desarrollar las habilidades y herramientas necesarias para recopilar rápidamente información clave, rastrear transacciones financieras casi instantáneas y recuperar activos virtuales antes de que se disipen. La naturaleza multidisciplinaria del ransomware también significa que las autoridades deben extender su colaboración más allá de sus contrapartes tradicionales para incluir agencias de ciberseguridad y protección de datos.

El GAFI también finalizó una lista de posibles indicadores de riesgo que pueden ayudar a las entidades del sector público y privado para identificar actividades sospechosas relacionadas con el *ransomware*.

La escala global de los flujos financieros relacionados con los ataques de *ransomware* ha crecido drásticamente en los últimos años. Las estimaciones de la industria informan un aumento de hasta cuatro veces en los pagos de *ransomware* en 2020 y 2021, en comparación con 2019. Las nuevas técnicas han aumentado la rentabilidad de los ataques y la probabilidad de éxito. Estos incluyen la orientación de entidades grandes y de alto valor, donde los delincuentes de *ransomware* venden *kits* de *software* fáciles de usar. Las consecuencias de los ataques de *ransomware* pueden ser nefastas y representar amenazas para la seguridad nacional, incluido el daño y la interrupción de infraestructura y servicios críticos.

Por medio del informe, el GAFI tiene como objetivo mejorar la comprensión global de los flujos financieros vinculados al *ransomware* y destacar las buenas prácticas para abordar esta amenaza. El informe también proporciona una lista de posibles indicadores de riesgo que ayudarán a las autoridades y al sector privado a detectar dichos flujos financieros. Los hallazgos de este informe se basan en la experiencia y los conocimientos de los sectores público y privado, incluidos los aportes y estudios de casos de más de 40 delegaciones en toda la Red Global de GAFI.

Un ataque de *ransomware* es una forma de extorsión y los Estándares del GAFI exigen que se tipifique como delito determinante del lavado de dinero.

El informe encuentra que los pagos y el lavado posterior de las ganancias del *ransomware* se realizan casi exclusivamente por medio de activos virtuales. Los delincuentes de *ransomware* explotan la naturaleza internacional de los activos virtuales para facilitar transacciones transfronterizas casi instantáneas a gran escala, a veces sin la participación de instituciones financieras tradicionales que tienen programas contra el Lavado de Dinero y el Financiamiento del Terrorismo (ALD/CFT). Los delincuentes complican aún más sus transacciones mediante el uso de tecnologías, técnicas que mejoran el anonimato en el proceso de lavado, como las criptomonedas mejoradas que difícilmente pueden ser rastreadas.

El uso casi exclusivo de activos virtuales en el lavado relacionado con *ransomware* refuerza aún más la importancia de acelerar la implementación de la *Recomendación 15* del GAFI, que requiere que las jurisdicciones implementen medidas para mitigar los riesgos relacionados con los activos virtuales y para regular el Proveedor de Servicios de Activos Virtuales (sector VASP). Estos esfuerzos son fundamentales para evitar que los delincuentes accedan fácilmente a los VASP ubicados en jurisdicciones con controles antilavado débiles o inexistentes para lavar las ganancias de sus delitos.

Este informe también encuentra que los ataques de *ransomware* generalmente no se denuncian, ya sea debido a desafíos en la detección por parte del sector privado, impactos negativos en el negocio de la víctima o temor a represalias de los delincuentes si una víctima informa un ataque. Esto explica en parte la falta de experiencia en la investigación de lavado de dinero relacionado con *ransomware*.

Las jurisdicciones deben realizar y fortalecer más el trabajo para aumentar y mejorar las fuentes de detección y notificación. Las autoridades deben moverse rápidamente para recopilar información clave y deben tener las herramientas y habilidades necesarias para rastrear y recuperar activos virtuales de manera efectiva

El *ransomware* atraviesa una amplia gama de áreas y las investigaciones pueden involucrar a actores fuera de las autoridades tradicionales en el combate al lavado de dinero y financiamiento al terrorismo, incluidas las agencias de ciberseguridad y protección de datos. Como tal, se requiere un enfoque multidisciplinario para abordar de manera efectiva este delito. Debido a la naturaleza inherentemente descentralizada y transnacional de los activos virtuales, es imperativo crear y aprovechar los mecanismos de cooperación internacional existentes para abordar con éxito el lavado relacionado con *ransomware*.

Ransomware es un tipo de *software* malicioso (*malware*) que los delincuentes desarrollan y/o utilizan para bloquear el acceso a datos, sistemas o redes mientras exigen el pago de un rescate a cambio. Los métodos de ataque comunes incluyen el cifrado de datos, la filtración de datos y la interrupción de las operaciones de las víctimas. Los ataques a menudo involucran más de un método y pueden incluir una amenaza para publicar los datos de la víctima.

Los incidentes de ransomware han crecido significativamente en los últimos años, tanto en número como en escala. El *ransomware* es principalmente un esfuerzo con fines lucrativos, y el crecimiento de los ataques ha llevado a un aumento consecuente en las ganancias para después ser lavadas.

Las estimaciones de la industria indican que los pagos de *ransomware* aumentaron al menos cuatro veces en 2020 y 2021 en comparación con 2019.

Si bien los últimos datos de la industria sugieren una tendencia a la baja en 2022 (posiblemente debido a la negativa de las víctimas a pagar), el valor de los activos virtuales recibidos por los atacantes de *ransomware* sigue siendo significativamente más alto que antes de 2019. Es probable que la cantidad total real de ataques y pérdidas relacionadas sea significativamente mayor, ya que los ataques de *ransomware* a menudo no se informan

Los ataques han causado importantes trastornos y daños a los gobiernos, las instituciones públicas, las empresas y los ciudadanos, en algunos casos afectando la atención médica y amenazando la seguridad nacional, lo que incluye la necesidad de detener infraestructura y servicios críticos o comprometer datos confidenciales.

Los delincuentes de *ransomware* han desarrollado técnicas para aumentar la rentabilidad de sus ataques y la probabilidad de éxito. Como resultado, la amenaza de flujos financieros ilícitos relacionados con *ransomware* probablemente seguirá creciendo.

Los delincuentes exigen pagos de *ransomware* casi exclusivamente en activos virtuales Las víctimas, o los terceros relacionados que actúan sobre una víctima, suelen utilizar VASP para pagar rescates. Los delincuentes de *ransomware* también utilizan VASP en los ataques a hospitales; por ejemplo, han puesto en peligro la atención de los pacientes y los ataques a los departamentos de policía que han visto afectada su seguridad.

"Proveedor de servicios de activos virtuales" significa cualquier persona física o jurídica que no esté cubierta en ninguna otra parte por las Recomendaciones, y como empresa realiza una o más de las siguientes actividades u operaciones para o en nombre de otra persona física o jurídica: intercambio entre activos virtuales y dinero fiduciario; monedas; intercambio entre una o más formas de activos virtuales; transferencia de activos virtuales; custodia y/o administración de activos virtuales o instrumentos que permitan el control de activos virtuales, y participación y provisión de servicios financieros relacionados con la oferta y/o venta de un activo virtual por parte de un emisor lavar fondos ilícitos e intercambiar ganancias por moneda fiduciaria, que se puede cambiar más fácilmente por bienes y servicios y es una reserva de valor más estable.

En 2018, el GAFI modificó sus Recomendaciones para cubrir los activos virtuales y los VASP. Desde entonces, el GAFI ha emitido varias guías para ayudar a las jurisdicciones y al sector privado a monitorear y mitigar los riesgos en este sector, incluidos los indicadores de alerta roja de LDFT. Si bien este trabajo a menudo se ha referido al *ransomware*, este informe es la primera vez que el GAFI se ha centrado específicamente en las tendencias y técnicas de lavado vinculadas a los ataques de *ransomware*.

El GAFI está aprovechando su experiencia en investigaciones financieras que involucran activos virtuales, para identificar desafíos y compartir buenas prácticas para contrarrestar los ataques de *ransomware*. Este informe se centra en cómo identificar y denunciar pagos relacionados con *ransomware*; prevenir, detectar e investigar los flujos financieros de *ransomware* y conocer el lavado de estos ingresos. Este informe no se centra en el uso de

ransomware para la financiación del terrorismo dada la falta de un uso significativo o notable de *ransomware* para este fin en la información y los estudios de casos presentados para este informe.

Debido a que un ataque de *ransomware* es una forma de extorsión, las recomendaciones del GAFI exigen que todas las jurisdicciones penalicen el LD relacionado con el *ransomware* (R.3). El GAFI también requiere que las jurisdicciones identifiquen, evalúen y tomen medidas para mitigar sus riesgos de LA (R.1-2); garantizar que el sector privado, incluidos los VASP, aplique medidas preventivas adecuadas, como informar transacciones sospechosas (R.9-23); avalar que las fuerzas del orden investiguen, rastreen y confisquen los productos delictivos (R.4, 29-31), y cooperar internacionalmente para perseguir el LD y los delitos determinantes, así como los activos asociados (R.36-40).

Si bien el *ransomware* es un tipo de delito cibernético, la información de este informe puede ser o no aplicable a otros tipos de delitos cibernéticos, como *malware*, *phishing*, compromiso de correo electrónico comercial o compromiso y venta de información financiera.

Debemos estar alertas, ya que podemos ser fácilmente víctimas de este delito.

Para descargar el informe completo dar clic aquí:

https://www.fatf-gafi.org/en/publications/Methodsandtrends/countering-ransomware-financing.html