REPORTE GAFI

Combate contra el financiamiento del *ransomware*

Marzo 2023

El Grupo de Acción Financiera (GAFI, o *FATF* por sus siglas en inglés) es un organismo intergubernamental independiente que desarrolla y promueve políticas para proteger al sistema financiero mundial del lavado de dinero, del financiamiento del terrorismo y de la financiación de armas de destrucción masiva. Las recomendaciones del GAFI son reconocidas como el estándar internacional anti-lavado de dinero y contra el financiamiento del terrorismo (ALD/CFT).

Para mayor información sobre el GAFI, consultar **www.fatf-gafi.org**

Referencia para citas:

GAFI (2023), *Countering Ransomware Financing,* FATF, Paris,
http://www.fatf-gafi.org/publications/Methodsandtrends/countering-*ransomware*-financing.html

Índice

Ver también:

Countering Ransomware Financing: Potential Risk Indicators (disponible en inglés)

Esta lista de posibles indicadores de riesgo complementa el informe del GAFI *Combate contra el Financiamiento del Ransomware* y puede ayudar a entidades de los sectores público y privado a identificar actividades sospechosas relacionadas con el *ransomware*.

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

Acrónimos

AEC	Criptomoneda con anonimato reforzado (*AEC, anonymity-enhanced cryptocurrency*)
ALD/CFT	Anti-lavado de dinero/contra-financiamiento del terrorismo (*AML/CFT, anti-money laundering/countering the financing of terrorism*)
CERT	Equipo de respuesta ante emergencias informáticas (*CERT, computer emergency response teams*)
DeFi	Finanza descentralizada (*DeFi, decentralized finance*)
APNFD	Actividades y profesiones no financieras designadas (*DNFBP, designated non-financial businesses and professions*)
UIF	Unidad de inteligencia financiera (*FIU, financial intelligence unit*)
IP	Protocolo de Internet (*IP, internet protocol*)
APJs	Autoridades de procuración de justicia (*LEA, law enforcement agency*)
LD	Lavado de dinero (*ML, money laundering*)
OTC	Operadores extrabursátiles (*OTC, over-the-counter*)
APP	Asociación público-privada (*PPP, public-private partnership*)
RaaS	*Ransomware* como servicio (*RaaS, ransomware as a service*)
ROS	Reporte de operaciones sospechosas (*STR, suspicious transaction report*)
VACG	Grupo de contacto de activos virtuales (*VACG, virtual asset contact group*)
PSAV	Proveedor de servicios de activos virtuales (*VASP, virtual asset service provider*)
VPN	Red privada virtual (*VPN, virtual private network*)

Resumen ejecutivo

La escala mundial de flujos financieros relacionados con ataques de *ransomware* (programas de secuestro de archivos) se ha incrementado dramáticamente en los últimos años. Las estimaciones de la industria reportan un aumento de hasta cuatro veces en los pagos de rescate por *ransomware* (pagos de rescate por secuestro de información) en 2020 y 2021, en comparación con 2019. Las nuevas técnicas han aumentado la rentabilidad de los ataques, así como sus probabilidades de éxito. Entre ellos se incluye la selección de entidades grandes de alto valor, así como el *ransomware* como un servicio (RaaS, por sus siglas en inglés), en el que los ciberdelincuentes de *ransomware* venden kits de software de fácil uso a los afiliados. Los ataques de *ransomware* pueden tener consecuencias graves y constituyen una amenaza para la seguridad nacional, ya que pueden dañar e interrumpir infraestructuras y servicios críticos.

A través del presente estudio, el GAFI pretende mejorar la comprensión global de los flujos financieros vinculados al *ransomware* y destacar las buenas prácticas para hacer frente a esta amenaza. El informe igualmente ofrece una lista de posibles indicadores de riesgo que ayudarán a las autoridades y al sector privado a detectar estos flujos financieros. Las conclusiones de este informe se basan en la experiencia y en los conocimientos de los sectores público y privado, incluyendo aportaciones y estudios de caso de más de 40 delegaciones de la red mundial del GAFI.

Un ataque de *ransomware* (ataque de secuestro de información) es una forma de extorsión y los Estándares del GAFI establecen que debe considerarse delito determinante del lavado de dinero (LD). Este informe concluye que los pagos y el posterior lavado de ganancias derivadas de un ataque por *ransomware* se realizan casi exclusivamente a través de activos virtuales. Los ciberdelincuentes de *ransomware* aprovechan la naturaleza internacional de los activos virtuales para facilitar transacciones transfronterizas a gran escala y casi instantáneas, a veces sin la participación de las instituciones financieras tradicionales que cuentan con programas anti-lavado de dinero y contra el financiamiento del terrorismo (ALD/CFT). Los ciberdelincuentes enmascaran aún más sus transacciones utilizando tecnologías, técnicas y tokens que, en el proceso de LD, favorecen el anonimato, tales como las AEC (criptomonedas con anonimato reforzado) y los mezcladores.

El uso casi exclusivo de activos virtuales en el lavado de ganancias provenientes de *ransomware* (ganancias derivadas de un ataque por secuestro de información) refuerza aún más la importancia de acelerar la aplicación de la Recomendación 15 del GAFI, la cual exige a las jurisdicciones establecer medidas para mitigar los riesgos vinculados a los activos virtuales y regular al sector de proveedores de servicios de activos virtuales (PSAV). Estos esfuerzos son fundamentales para impedir que los ciberdelincuentes accedan fácilmente a los PSAV ubicados en jurisdicciones con controles ALD/CFT débiles o inexistentes para lavar las ganancias procedentes de sus delitos.

El presente informe también revela que los ataques de *ransomware* por lo general no se denuncian, ya sea porque son difíciles de detectar por parte del sector privado, por las repercusiones negativas que representan para el negocio de la víctima o por miedo a represalias por parte de los ciberdelincuentes cuando una víctima denuncia un ataque. Esto explica, en parte, la falta de experiencia en la investigación de LD relacionado con el *ransomware*. Las jurisdicciones deben continuar en sus esfuerzos para ampliar y mejorar las fuentes de detección y denuncia. Las autoridades deben actuar con rapidez para recopilar información clave así como contar con las herramientas y habilidades necesarias para rastrear y recuperar eficazmente los activos virtuales.

El *ransomware* afecta a una amplia gama de sectores y las investigaciones pueden implicar a agentes más allá de las autoridades tradicionales de ALD/CFT y los organismos de ciberseguridad y protección de datos. Por ello se requiere un enfoque multidisciplinario

para abordar eficazmente tanto al *ransomware* como al LD asociado a este. Debido a la naturaleza intrínsecamente descentralizada y transnacional de los activos virtuales, es imperativo construir y aprovechar los mecanismos de cooperación internacional existentes para combatir con éxito el LD relacionado con el *ransomware*.

Para reforzar la respuesta global contra el *ransomware* y el LD relacionado con este, el GAFI propone que las jurisdicciones establezcan las siguientes medidas.

Acciones sugeridas

La información recopilada para el presente estudio proporcionó algunos ejemplos prácticos de medidas que los países pueden adoptar para mejorar su capacidad para contrarrestar los flujos financieros ilícitos relacionados con el *ransomware*. En esta sección se resumen dichas buenas prácticas y se mencionan sugerencias sobre la forma en que las jurisdicciones podrían atacar más eficazmente el LD relacionado con el *ransomware*.

Implementar los Estándares del GAFI, incluyendo los correspondientes a los PSAV, y mejorar la detección

- Las jurisdicciones deberían agilizar el cumplimiento de los Estándares del GAFI sobre el sector PSAV aplicando la Recomendación 15 (incluida la regla de viaje[1]) lo antes posible. Esto garantizaría que los PSAV cumplen con las obligaciones necesarias en materia de ALD/CFT para recopilar información financiera crítica y denunciar operaciones sospechosas.
- Las jurisdicciones deben asegurarse de que el *ransomware* sea considerado un delito de LD en línea con la Recomendación 3 del GAFI (por ejemplo, clasificándolo como un tipo de extorsión).
- Las jurisdicciones deben mejorar la detección de *ransomware*:
    - Apoyando a las entidades reguladas para que detecten el *ransomware* y el LD asociado a este y denuncien transacciones sospechosas, por ejemplo, informando sobre tendencias, guías de detección e indicadores de alerta (como los que se mencionan en *Countering Ransomware Financing: Potential Risk Indicators*[2]) con los sujetos obligados pertinentes.
    - Alentando a las víctimas a denunciar voluntariamente los incidentes, por ejemplo, dando a conocer los apoyos y recursos disponibles o creando canales seguros para realizar denuncias.
- Las jurisdicciones igualmente deben considerar la posibilidad de establecer canales de comunicación con agentes no tradicionales que puedan no estar sujetos a la regulación de ALD/CFT (como las compañías de ciberseguros y empresas de respuesta a incidentes) para ampliar las fuentes de detección.

Promover las investigaciones financieras y los esfuerzos de recuperación de activos

- Las autoridades competentes deben utilizar y adaptar, según sea necesario, las técnicas tradicionales de las APJs, así como las técnicas

1 La "regla de viaje" es una medida clave en materia de ALD/CFT que obliga a los PSAV a obtener, conservar e intercambiar información sobre los remitentes y beneficiarios de transferencias de activos virtuales, permitiendo tanto a instituciones financieras como a los PSAV realizar un control de las sanciones y detectar transacciones sospechosas.

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

específicas de los activos virtuales, para llevar a cabo investigaciones de LD relacionadas con el *ransomware*. Las autoridades competentes deben contar con las habilidades y los conocimientos especializados necesarios para llevar a cabo de manera exitosa investigaciones financieras sobre *ransomware*. Esto incluye el desarrollo, acceso, así como la capacitación relacionada con herramientas de análisis y supervisión de cadenas de bloques.

- Las jurisdicciones deben garantizar que las APJs establezcan y mantengan vigentes las habilidades y facultades necesarias para asegurar y confiscar activos de forma rápida y eficaz, especialmente en el caso de activos virtuales. Las jurisdicciones deben garantizar la existencia de mecanismos especializados para gestionar adecuadamente los activos virtuales asegurados.

Adoptar un enfoque multidisciplinario para combatir al *ransomware*

- Las jurisdicciones deben asegurarse de identificar y evaluar los riesgos de LD provenientes del *ransomware* en sus evaluaciones de riesgo país, considerando la naturaleza descentralizada tanto de los activos virtuales como de los grupos delictivos dedicados al *ransomware*, incluyendo jurisdicciones con sectores de activos virtuales en los que el *ransomware* aún no sea considerado una amenaza a la seguridad nacional. Los resultados de estas evaluaciones pueden ayudar a reforzar las estrategias nacionales de ciberseguridad mediante la aplicación de un enfoque global de riesgos relacionados con el *ransomware*.

- Las jurisdicciones deben desarrollar mecanismos de coordinación entre las autoridades competentes, desde APJs, ALD/CFT y las dedicadas a atacar el cibercrimen, hasta socios no tradicionales, como las agencias de ciberseguridad o de protección de datos. Esto fomenta el intercambio de información e inteligencia y constituye una plataforma útil para el intercambio de conocimientos técnicos especializados.

Apoyar la colaboración con el sector privado

- Las jurisdicciones deben identificar y establecer mecanismos que promuevan la cooperación entre los sectores público y privado. Las jurisdicciones deben considerar incluir a los PSAV así como a otros socios no tradicionales en dichos mecanismos de cooperación para crear plataformas útiles a fin de incrementar la concientización, intercambio de conocimientos e ideas y así contribuir a los objetivos de las APJs.

Mejorar la cooperación internacional

- Las jurisdicciones deben establecer mecanismos bilaterales, regionales y multilaterales y participar activamente en ellos, por ejemplo, mediante el establecimiento de oficinas de enlace y puntos de contacto transparentes 24 horas al día, 7 días a la semana, para facilitar la cooperación internacional y un rápido intercambio de información. Esto ayudaría a rastrear fondos transfronterizos con rapidez, recuperar activos de forma eficaz, y a que las autoridades puedan desmantelar exitosamente las redes transnacionales vinculadas al *ransomware* y al LD relacionado con este.

Introducción

Objetivos y alcance

1. El *ransomware* es un tipo de malware que los delincuentes desarrollan y/o utilizan para denegar el acceso a datos, sistemas o redes, exigiendo a cambio el pago de un rescate. Los métodos de ataque más comunes incluyen el cifrado de datos, la exfiltración de datos y la interrupción de actividades de las víctimas. Los ataques suelen incluir más de un método, así como la amenaza de publicar los datos de la víctima.[3]
2. Los incidentes de *ransomware* han aumentado considerablemente en los últimos años[4], tanto en número como en escala. El *ransomware* es, ante todo, una actividad con fines lucrativos y el aumento de los ataques ha conllevado un incremento en ganancias derivadas tanto de los ataques como del LD relacionado con los mismos. Las estimaciones del sector indican que los pagos de rescate por *ransomware* casi se cuadriplicaron en 2020 y 2021 en comparación con 2019.[5] Si bien los últimos datos de la industria sugieren una tendencia a la baja en 2022 (en gran medida debido a la negativa de las víctimas a pagar), el valor de los activos virtuales recibidos por perpetradores de ataques de *ransomware* sigue siendo significativamente mayor que antes de 2019.[6] Es probable que el número total real de ataques y pérdidas relacionadas sea considerablemente mayor, ya que los ataques de *ransomware* a menudo no se denuncian.
3. Los ataques han ocasionado disrupciones y daños considerables en gobiernos, instituciones públicas, empresas y ciudadanos, afectando en algunos casos a los sistemas de salud y amenazando la seguridad nacional, incluso paralizando infraestructuras y servicios críticos o comprometiendo datos sensibles.[7] Los ciberdelincuentes de *ransomware* han desarrollado técnicas para aumentar la rentabilidad de sus ataques y las probabilidades de éxito. En consecuencia, la amenaza de flujos financieros ilícitos relacionados con el *ransomware* muy probablemente continúe incrementándose.
4. Los ciberdelincuentes exigen el pago de rescate por *ransomware* casi siempre en activos virtuales. Las víctimas, o terceros relacionados que actúan por cuenta de una víctima, suelen recurrir a los PSAV[8] para pagar los rescates. Los delincuentes de *ransomware* utilizan a los PSAV para lavar fondos ilícitos y canjear las ganancias por moneda fiduciaria, la cual es fácilmente intercambiable por bienes y servicios y constituye un depósito de valor más estable.

---

3 FBI *Scams and Safety: Ransomware* (consultado en septiembre 2022, disponible en inglés): www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware; *Australian Cyber Security Centre Ransomware* (consultado en septiembre 2022, disponible en inglés): www.cyber.gov.au/*ransomware*.

4 ENISA *Threat Landscape 2022* (octubre 2022), disponible en inglés en www.enisa.europa.eu/publications/enisa-threat-landscape-2022

5 Chainalysis, *Chainalysis Crypto Crime Report 2022* (febrero 2022), disponible en inglés en: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

6 Chainalysis, *Ransomware Revenue Down As More Victims Refuse to Pay* (enero 2023), disponible en inglés en: https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down- as-victims-refuse-to-pay/

7 Los ataques a hospitales, por ejemplo, han puesto en peligro la atención a pacientes, y los ataques a sectores de procuración de justicia han afectado la seguridad interna de los países.

8 Por PSAV se refiere a cualquier persona física o jurídica que no se encuentre incluida en ningún otro apartado de las Recomendaciones, y que cómo empresa realiza una o varias de las siguientes actividades u operaciones para o en nombre de otra persona física o jurídica: intercambio de activos virtuales y monedas fiduciarias; intercambio de una o varias formas de activos virtuales; transferencia de activos virtuales; gestión y/o custodia de activos virtuales o instrumentos que permitan el control de activos virtuales; y participación en y prestación de servicios financieros relacionados con la oferta y/o venta de un activo virtual por parte de un emisor.

5. En 2018, el GAFI modificó sus Recomendaciones para incluir tanto a activos virtuales como a los PSAV. Desde entonces, el GAFI ha publicado diversas guías para ayudar a las jurisdicciones y al sector privado a vigilar y mitigar los riesgos en esta materia, así como indicadores de alerta de LD y financiación del terrorismo (FT).[9] Aunque dichos trabajos frecuentemente han abordado el *ransomware*, a partir del presente informe es la primera vez que el GAFI se enfoca específicamente en las tendencias y técnicas de LD relacionadas con ataques de *ransomware*.
6. Bajo la Presidencia de Singapur, el GAFI está aprovechando su experiencia en investigaciones financieras relacionadas con activos virtuales, para identificar retos y compartir buenas prácticas para contrarrestar el financiamiento del *ransomware* y el LD relacionado a este. El presente informe se enfoca en: cómo detectar y reportar los pagos relacionados con *ransomware*; cómo prevenir, detectar e investigar los flujos financieros provenientes del *ransomware*; y cómo se blanquean dichos ingresos. El presente informe no se enfoca en el uso de *ransomware* para la financiación del terrorismo, ya que la información y los estudios de caso presentados en este informe no revelan un uso significativo o notable de *ransomware* para dicho propósito.
7. Dado que un ataque de *ransomware* es una forma de extorsión, las Recomendaciones del GAFI establecen que todas las jurisdicciones deben criminalizar el LD relacionado con el *ransomware* (R.3). El GAFI también requiere a las jurisdicciones identificar, evaluar y establecer medidas para mitigar los riesgos de LD (R.1-2); que el sector privado, incluyendo los PSAV, adopten medidas preventivas adecuadas, como denunciar operaciones sospechosas (R.9-23); que las APJs investiguen, rastreen y confisquen el producto del delito (R.4, 29- 31); y establecer medidas de cooperación internacional para combatir el LD y los delitos determinantes, así como las ganancias asociadas (R.36-40).
8. Aunque el *ransomware* es un tipo de ciberdelito, el presente informe se centra únicamente en información sobre *ransomware* y puede o no ser aplicable a otros tipos de ciberdelito, como el malware y el *phishing* para comprometer correos electrónicos relacionados con transacciones comerciales o para vender información financiera.

Objetivos y estructura

9. La sección I de este informe detalla cómo los ciberdelincuentes de *ransomware* reciben, lavan y hacen efectivas sus ganancias ilícitas. El objetivo de dicha sección es lograr una mayor concientización y comprensión de la magnitud de la amenaza mundial que el *ransomware* representa, cómo se efectúan los pagos por *ransomware* o relacionados con este, y cómo los ingresos relacionados con ataques de *ransomware* son canalizados a los ciberdelincuentes.
10. La sección II identifica los retos y las buenas prácticas en materia de identificación, investigación e interrupción de flujos financieros relacionados con el *ransomware*.
11. Este informe tiene como objetivo ayudar a las **autoridades operativas** a generar inteligencia financiera de alta calidad, realizar investigaciones financieras e identificar, rastrear y asegurar ingresos ilícitos. Los **reguladores** y **responsables de políticas nacionales** pueden utilizar la información del presente informe para identificar vulnerabilidades y mitigar riesgos. Dicha información también ayudará a las **instituciones financieras**, a los **PSAV** y a las **APNFD** a diseñar y a aplicar controles para detectar, informar y prevenir el movimiento ilícito de ingresos relacionados con el *ransomware*.

[9] FATF (junio 2022) *Targeted Update on Implementation of the FATF Standards on Virtual Assets And Virtual Asset Service Providers;* (septiembre 2020) *Virtual Assets Red Flag Indicators*; y (agosto 2019) *Confidential FATF Guidance on Financial Investigations Involving Virtual Assets*, disponibles en inglés.

Metodología

12. Este proyecto fue dirigido conjuntamente por expertos de Israel y Estados Unidos. Las siguientes jurisdicciones y entidades igualmente participaron en el equipo del proyecto: Alemania, Australia, Canadá, la Comisión Europea, España, Filipinas, Francia, Japón, Luxemburgo, México, Reino Unido, Singapur, Sudáfrica, Suiza, Turquía, el Grupo Asia-Pacífico sobre Lavado de Activos, y el Grupo Egmont de Unidades de Inteligencia Financiera.

13. Las conclusiones del presente informe se basan en:

- Una revisión de la literatura existente, así como de material de libre acceso sobre este tema.
- Una petición a la Red Global del GAFI de más de 200 jurisdicciones para obtener información sobre las percepciones de riesgo, leyes y facultades nacionales, los retos y buenas prácticas, así como estudios de caso relacionados con el *ransomware* en cada jurisdicción. En total, el equipo del proyecto recibió información de más de 40 delegaciones.
- Las discusiones generadas en el Grupo de Contacto de Activos Virtuales del GAFI (VACG).[10]
- La colaboración con el sector privado realizada a través del VACG.

[10] En junio de 2019, el Grupo de Desarrollo de Políticas (PDG) acordó crear el VACG para informar al sector privado sobre los requerimientos del GAFI y garantizar que el primero desarrolle soluciones tecnológicas apropiadas para implementar rápidamente dichos requerimientos.

SECCIÓN I. FLUJOS FINANCIEROS PROVENIENTES DEL *RANSOMWARE*

Magnitud de flujos financieros

14. La escala de los ataques de *ransomware*, así como los flujos financieros relacionados con este, se han incrementado de manera alarmante en todo el mundo. Muchas jurisdicciones han registrado un aumento en la frecuencia de los ataques de *ransomware* en los últimos años que oscila entre 10% y varios cientos por ciento, dependiendo de la jurisdicción. Se ha registrado un incremento en denuncias por parte de las víctimas, así como en reportes de operaciones sospechosas (ROS) relacionadas con el *ransomware* en diversas jurisdicciones. En una jurisdicción, los ROS presentados en los primeros seis meses de 2021 identificaron el equivalente a 590 millones de dólares (552 millones de euros) en transacciones relacionadas con *ransomware*, un aumento de 42% en comparación con 2020, cuando el total alcanzó 416 millones de dólares (389 millones de euros).[11] Los informes anuales recientes de las APJ muestran un aumento significativo en la actividad de *ransomware*[12], y las estimaciones del sector muestran un crecimiento similar en cuanto al número de ataques y variantes activas de *ransomware*. En 2021, el número estimado de ataques de *ransomware* era de alrededor de 623,3 millones, más del doble que los 304,6 millones de ataques estimados en 2020.[13] De igual manera, el número estimado de variantes activas de *ransomware* se ha duplicado con respecto a 2019.[14]

15. Aunque ciertas jurisdicciones declararon niveles bajos de ataques de *ransomware*, la información recopilada para el presente informe muestra que los ataques de *ransomware* no se denuncian completamente, a pesar de que el número de ROS y de denuncias por parte de las víctimas ha aumentado en algunas jurisdicciones. Ello dificulta estimar de manera precisa el número total de incidentes y de cantidades pagadas por concepto de rescate. Los estudios de caso presentados en este informe mostraron que el *ransomware* puede ser un riesgo tanto para jurisdicciones desarrolladas como en vías de desarrollo, independientemente de la región.

16. Varias jurisdicciones identificaron que el incremento tanto en ataques de *ransomware* como en flujos financieros relacionados está asociado al desarrollo de técnicas por parte de los ciberdelincuentes de *ransomware* como **las técnicas de ciberataque de alto perfil, el RaaS, las tácticas de doble/triple/múltiple extorsión** para maximizar la eficacia de los ataques, y las ganancias resultantes (ver Recuadro 1).

---

11 FINCEN, *Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021* (junio 2021), disponible en inglés en: www.fincen.gov/sites/default/files/2021-10/Financial Trend Analysis Ransomware 508 FINAL.pdf

12 FBI, *Internet Crime Report 2021* (consultado el 1 de diciembre 2022), disponible en inglés en: www.ic3.gov/Home/AnnualReports; EUROPOL, *Internet Organised Crime Threat Assessment (IOCTA) 2021* (consultado el 1 de diciembre 2022), disponible en inglés en: www.europol.europa.eu/publications-events/main-reports/iocta-report

13 SonicWall, *2022 SonicWall Cyber Threat Report* (2022), disponible en inglés en: www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf

14 Chainalysis, *Chainalysis Crypto Crime Report 2022* (febrero 2022), disponible en inglés en: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

Recuadro 1. Desarrollo de técnicas de *ransomware*

En el caso de **las técnicas de ciberataque de alto perfil**, los ciberdelincuentes de *ransomware* establecen como objetivo de ataque grandes organizaciones de alto valor o entidades de alto perfil que consideran son más propensas a pagar un rescate ya sea para reanudar sus operaciones comerciales o para evitar el escrutinio público. Los ciberdelincuentes de *ransomware* igualmente atacan de forma selectiva a organizaciones que operan en cadenas de suministro "justo a tiempo" y que tienen más probabilidades de sufrir mayores costos por tiempo de inactividad, como a infraestructuras críticas y organizaciones que poseen información sensible o valiosa. Los ciberatacantes consideran que este tipo de organizaciones son más propensas a pagar rescates que otras víctimas.

RaaS hace referencia a un modelo de negocio delictivo en el que los delincuentes de *ransomware* proporcionan kits de software de *ransomware* en la *dark web* o subcontratan elementos de ataque de *ransomware*, incluyendo la distribución de malware, el compromiso inicial de la red de una víctima, la exfiltración de datos o la negociación de rescates para afiliados a cambio de una tarifa y/o un porcentaje del rescate. Los ciberdelincuentes también pueden adquirir credenciales robadas para acceder a los sistemas de las víctimas y explotarlos, lo que permite la propagación del *ransomware*, y pueden obtener información sobre sectores específicos en determinadas jurisdicciones para focalizar sus objetivos y maximizar la eficacia de sus ataques. El modelo RaaS ha reducido el costo y la experiencia técnica requerida para llevar a cabo ataques de *ransomware*, reduciendo las barreras de entrada y permitiendo a delincuentes menos sofisticados realizar ataques de *ransomware*.

La doble extorsión se refiere a una práctica en la que los operadores de *ransomware* exfiltran los datos de una víctima previo a cifrarlos y posteriormente amenazan con publicar los datos robados si no se satisfacen las peticiones de rescate. Esta amenaza de publicación se suma a la amenaza de mantener el sistema interrumpido. Esta táctica puede ejercer una presión adicional sobre las víctimas para que paguen las peticiones de rescate, aun cuando las víctimas sean capaces de restablecer sus operaciones.

La triple extorsión se refiere a una práctica en la que los operadores de *ransomware* buscan dinero no sólo de la víctima que fue el primer objetivo, sino de otra que podría verse afectada por la divulgación de datos de la primera víctima objetivo, como información médica protegida, información personal identificable, credenciales de sus cuentas e información relacionada con propiedad intelectual**.**

La extorsión múltiple se refiere a una práctica que implica más de dos métodos de extorsión. Se basa en la doble extorsión mediante cifrado y exfiltración, pero incluye tácticas de presión adicionales, como la denegación de servicio distribuido (DDoS, por sus siglas en inglés), el contacto con los clientes de las víctimas, la venta al descubierto de acciones de las víctimas, y la interrupción de los sistemas de infraestructura.

17. De acuerdo con información pública, más de la mitad de los ataques de *ransomware* denunciados están dirigidos a víctimas del sector público, de la salud y del de bienes y servicios industriales[15, 16.] Es probable que esto se deba en parte a las técnicas de ciberataque de alto perfil, para explicar los grandes pagos y el incremento general en pagos de rescate por *ransomware*. En los últimos años, los delincuentes de *ransomware* también han vulnerado instituciones energéticas, financieras, de comunicación y educativas. Aunque los ciberdelincuentes que emplean tácticas de ciberataque de alto perfil pueden centrarse en víctimas de alto perfil, las organizaciones e industrias medianas y pequeñas también se encuentran sujetas a extensos ataques de *ransomware*. De hecho, los ataques de *ransomware* siguen teniendo como principal objetivo a las pequeñas y medianas empresas. Lo anterior puede tener una relación riesgo/beneficio más consistente en comparación con los ataques de alto perfil contra víctimas de mayor tamaño. En el segundo trimestre de 2020, casi 55% de la totalidad de dichos ataques se produjo contra empresas con menos de 100 empleados, y cerca de 75% de los ataques se registró contra empresas con menos de 50 millones de dólares (47 millones de euros) de ingresos[17].

18. Los importes de rescate oscilan entre los cientos de dólares o euros en activos virtuales en casos de pequeña escala dirigidos a particulares hasta el equivalente a millones de dólares o euros en casos dirigidos a grandes empresas, especialmente a infraestructuras críticas u organizaciones que poseen información sensible o valiosa. La experiencia de las jurisdicciones indica que el importe de los rescates solicitados por los ciberdelincuentes también se ha incrementado en los últimos años. En 2021, el pago promedio de rescate rondó en 800,000 dólares (748,000 euros) en activos virtuales, casi cinco veces más que en 2020[15]. Es probable que este aumento se encuentre relacionado con el uso de técnicas de ciberataque de alto perfil, mencionadas anteriormente. En algunos casos, las peticiones de rescate han alcanzado decenas de millones de dólares o euros en activos virtuales. Por ejemplo, según informes de prensa, en 2021, una compañía de seguros con sede en EE.UU. fue atacada por un *Phoenix CryptoLocker* (al parecer, el tercer mayor RaaS en ingresos en 2021 después de *Conti* y *DarkSide*)[18] y al parecer pagó 40 millones de dólares (37 millones de euros) para recuperar el control de su red[19].

---

15 Sophos, *The State of Ransomware in State and Local Government* (septiembre 2022), disponible en inglés en: https://assets.sophos.com/X24WTUEQ/at/rbjqpp5wwm6v5h3wj9v3733/sophos-state- of-*ransomware*-government-2022-wp.pdf.

16 Digital Shadows, *Ransomware: Analyzing The Data From 2020* (enero), disponible en inglés en: www.digitalshadows.com/blog-and-research/ransomware-analyzing-the-data-from- 2020/.

17 Coveware, *Q2 Quarterly Report* (agosto 2020), disponible en inglés en: www.coveware.com/blog/q2-2020-ransomware-marketplace-report.

18 Chainalysis, *Chainalysis Crypto Crime Report 2022* (febrero 2022), disponible en inglés en: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

19 Mehrotra, Kartikay and Turton, William, *CNA Financial Paid $40 Million in Ransom After March Cyberattack*, Bloomberg, 20 de mayo 2021 (consultado el 1 de diciembre de 2022), disponible en inglés en: www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

Características y tendencias geográficas

19. En general, el *ransomware* es un fenómeno internacional que surge por la naturaleza misma tanto del ciberdelito como de los activos virtuales. La información de la Red Mundial del GAFI, los estudios de caso y los datos del sector revelan ciertas características y tendencias geográficas en los ataques de *ransomware*. Numerosas redes de *ransomware* han estado vinculadas a jurisdicciones con mayor riesgo de LD (ver Recuadro 2). En muchos casos, los ciberdelincuentes de *ransomware* depositan o cobran sus ganancias en estas jurisdicciones. En otros casos, los ataques de *ransomware* se realizan desde estas jurisdicciones o son potencialmente financiados por ellas.[20]

Recuadro 2. Jurisdicciones con mayor riesgo de lavado de dinero

Aunque no existe una definición o metodología universalmente aceptada para determinar si una jurisdicción representa un mayor riesgo de LD/FT, la consideración de los riesgos específicos de cada país, junto con otros factores de riesgo, proporciona información útil para determinar con mayor precisión los riesgos potenciales de LD/FT. Los indicadores de mayor riesgo incluyen: (a) países o zonas geográficas identificados por fuentes fidedignas como proveedores de financiamiento o apoyo a actividades terroristas o que cuentan con organizaciones terroristas designadas que operan en ellos; (b) países identificados por fuentes fidedignas como países con altos índices de delincuencia organizada, corrupción u otras actividades delictivas, incluyendo países de origen o tránsito de drogas ilegales, trata de personas, contrabando y juego ilegal; (c) países sujetos a sanciones, embargos o medidas similares dictadas por organizaciones internacionales como las Naciones Unidas; y (d) países identificados por fuentes fidedignas como países con regímenes de gobernanza, procuración de justicia y regulación débiles, incluyendo países identificados por las declaraciones del GAFI como países con regímenes débiles de ALD/CFT, especialmente para los PSAV, y para los cuales los PSAV y otras entidades obligadas deben prestar especial atención a relaciones y transacciones comerciales.

Fuente: FATF (2021) *Updated Guidance for a Risk-Based Approach: Virtual Assets and VASPs*, p. 154, disponible en inglés.

20. La magnitud de ataques de *ransomware* varía según la ubicación geográfica. Los informes del sector de 2022 indican que la región de Medio Oriente y África fue la menos afectada por dichos ataques (4%), seguida de América Latina (6%), Asia-Pacífico (10%), Europa (28%) y América del Norte (52%).[21] La variación en escala entre regiones geográficas ha tenido un impacto en cómo estas últimas perciben el riesgo al que se enfrentan por *ransomware*. La información proporcionada por la Red Global del GAFI muestra que las jurisdicciones que registran un aumento en técnicas de ciberataque de alto perfil y en rescates de alto valor asociados son más propensas a evaluar los riesgos de LD asociados con *ransomware* como altos.

---

20 *Alert (AA22-187A) from the U.S. Cybersecurity & Infrastructure Security Agency* (julio 2022), disponible en inglés en: www.cisa.gov/uscert/ncas/alerts/aa22-187a.

21 Group-IB, *Ransomware Uncovered Report. Group-IB* (mayo 2022), disponible en inglés en: https://spiresolutions.com/wp- content/uploads/2021/07/ransomware_uncovered_2020.pdf.

21. Muchos grupos importantes de *ransomware* utilizan una versión de RaaS denominada modelo de afiliación, en la que subcontratan elementos que realizan el ataque de *ransomware* a cambio de una cuota y/o un porcentaje del rescate. En dichos casos, estos delincuentes suelen estar dispersos geográficamente, por lo que puede resultar difícil lograr su identificación y detectar su ubicación. Por ejemplo, como muestra el estudio de caso de EMOTET (ver Recuadro 3), los delincuentes de *ransomware* pueden colaborar en la ejecución de los ataques o utilizar infraestructuras compartidas operando desde distintas jurisdicciones. La variedad de ciberdelincuentes implicados en diversas jurisdicciones puede igualmente dificultar el rastreo de flujos de dinero asociados a los principales delincuentes de *ransomware*.

Recuadro 3. Estudio de caso EMOTET[1]

EMOTET es una de las campañas de malware más importantes de los últimos años. Fue descubierto por primera vez en 2014 como un virus troyano bancario[2], convirtiéndose en una herramienta clave para otros malware y *ransomware*. En el momento del desmantelamiento de la red en enero de 2021, EMOTET era responsable de hasta 70% de los malware del mundo, incluyendo *RYUK* y *DoppelPaymer*, que han tenido un impacto económico significativo en las empresas del Reino Unido. En el operativo colaboraron estrechamente las APJs de Alemania, Canadá, Estados Unidos, Francia, Lituania, Países Bajos, Reino Unido y Ucrania, bajo la coordinación internacional de Europol y Eurojust. Gracias a dicha colaboración, las APJs nacionales lograron localizar y analizar los datos que vinculaban los datos de pago y registro con los delincuentes que utilizaban EMOTET. El caso ilustra la magnitud y la naturaleza del ciberdelito, y demuestra la importancia de la cooperación internacional para afrontar esta amenaza.

Fuente: Reino Unido.

Notas:
1. Comunicado de prensa de Europol sobre EMOTET, disponible en inglés en: www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
2. Un troyano bancario es un programa malicioso que intenta robar las credenciales de los clientes de una institución financiera o acceder a su información financiera.

22. El lavado de pagos de rescate por *ransomware* también es transnacional, dada la naturaleza transfronteriza de los activos virtuales en los que casi siempre se realizan los pagos de rescate por *ransomware*. Los usuarios de activos virtuales pueden realizar transacciones de par a par, es decir, directamente entre sí, utilizando únicamente su clave privada y una conexión a Internet, independientemente de las fronteras geográficas y sin la intervención de instituciones con obligaciones de ALD/CFT. Los delincuentes, incluyendo a los criminales de *ransomware* con acceso a Internet, pueden explotar las características de los activos virtuales para facilitar transacciones transfronterizas a gran escala, casi instantáneas y sin intermediarios financieros tradicionales que cuenten con programas de ALD/CFT. Igualmente tienen acceso a los PSAV situados en todo el mundo en jurisdicciones con controles ALD/CFT débiles o inexistentes, que los delincuentes de *ransomware* utilizan para cobrar sus ganancias ilícitas en moneda fiduciaria.

Recuadro 4. ¿Qué es un activo virtual?

Un activo virtual es una representación digital de valor que puede comercializarse o transferirse digitalmente y utilizarse para pagos o inversiones. Los activos virtuales no incluyen las representaciones digitales de las monedas fiduciarias, los valores u otros activos financieros contemplados en otras Recomendaciones del GAFI.

Los activos virtuales más utilizados son un medio de intercambio, para cuya generación o registros de propiedad se recurre a una tecnología de contabilidad distribuida (DLT) basada en la criptografía, como las cadenas de bloques (*blockchains*). Como se explica más adelante en este documento, muchos activos virtuales populares operan en cadenas de bloques públicas, en las que puede visualizarse información sobre transacciones seudónimas.

Fuente: GAFI.

Métodos y tendencias comunes

23. Para realizar una investigación financiera sobre un ataque de *ransomware* de manera exitosa es necesario conocer a fondo los métodos y técnicas utilizados para lavar fondos. Dado que los ataques de *ransomware* no suelen ser debidamente denunciados, este informe recopiló información de diversas fuentes abiertas, así como la experiencia de las jurisdicciones, para comprender mejor cómo se efectúan, lavan, reciben y, en algunos casos, intercambian los pagos de rescates por moneda fiduciaria.

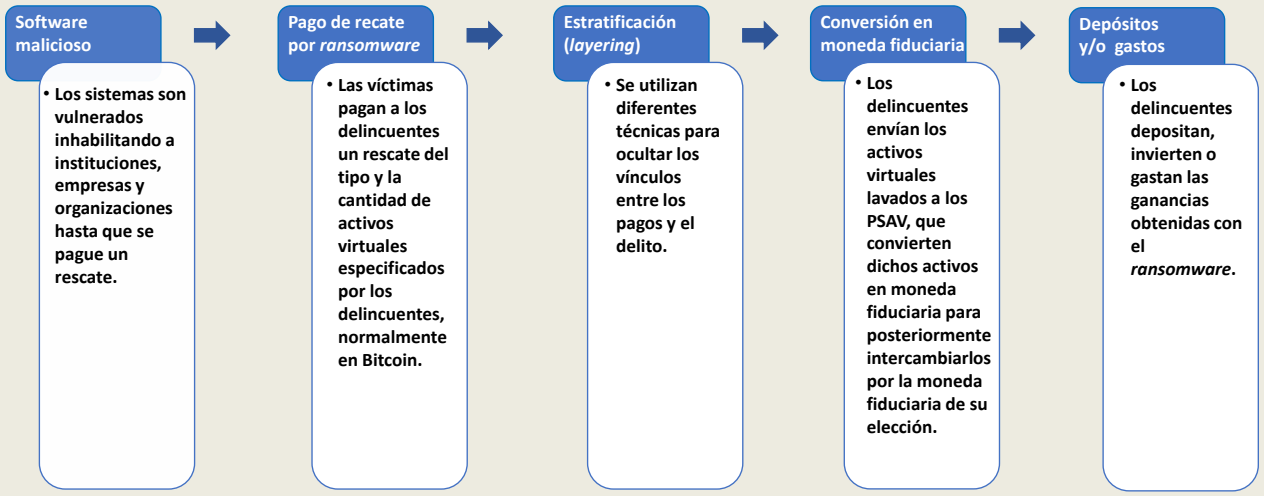
24. Los flujos financieros relacionados con *ransomware* suelen implicar a múltiples instituciones financieras tradicionales, así como a los PSAV. Otros terceros, como compañías de ciberseguros, empresas de respuesta a incidentes o empresas de ciberseguridad, también pueden participar en la respuesta a un ataque de *ransomware*, incluyendo el proceso de pago de las víctimas.

25. Aunque los activos virtuales son el principal método de pago de rescate por *ransomware*, los flujos financieros globales relacionados con este mismo involucran a múltiples instituciones financieras tradicionales, así como a los PSAV y a otras terceras partes.

Cuadro 1. Tipos de sectores que pudieran estar implicados en los flujos financieros relacionados con el *ransomware*

Instituciones financieras	Las instituciones financieras suelen actuar como intermediarios utilizados por las víctimas de *ransomware* (o un tercero que opera en nombre de la víctima) para transferir fondos a un PSAV para adquirir activos virtuales.
PSAV	Las víctimas (o un tercero que opera en nombre de la víctima) de *ransomware* utilizan los PSAV para comprar y transferir el tipo y la cantidad de activos virtuales especificados por el delincuente de *ransomware*.
Compañías de seguros	Las compañías de seguros pueden cubrir y a veces pagar el rescate como parte de la cobertura de ciberseguro.
Empresas de respuesta a incidentes	Las empresas de respuesta a incidentes contratadas por las víctimas de *ransomware* suelen negociar el pago del rescate con los ciberdelincuentes responsables del ataque. Como parte de su servicio, dichas empresas pueden comprar los activos virtuales a los PSAV para pagar el rescate y transferirlos a los ciberdelincuentes responsables del ataque en nombre de las víctimas.
Compañías de ciberseguros	Empresas responsables de salvaguardar los datos, sistemas, redes y dispositivos conectados del cliente de cualquier acceso no autorizado e ilegal.

Recuadro 5. Flujos financieros típicos relacionados con pagos de rescate por *ransomware*



Posterior a la recepción de la petición de rescate por parte de la víctima, esta última o un tercero que opera en su nombre suele transmitir los fondos mediante una transferencia bancaria, una cámara de compensación automatizada (CCA) o un pago con tarjeta de crédito a un PSAV para comprar el tipo y la cantidad de activo virtual especificado por el ciberdelincuente de *ransomware*. Terceros que operan en nombre de la víctima pueden ser empresas de respuesta a incidentes o de ciberseguros.

Posteriormente, la víctima o un tercero envía el pago del rescate, a menudo desde un monedero alojado en un PSAV, a la dirección del activo virtual del agresor. Por lo general se trata de una billetera no alojada (un software o hardware que permite a los usuarios tener, almacenar y transferir activos virtuales de forma autónoma a un tercero, como un PSAV; también denominado monedero no custodiado) controlado por un ciberdelincuente de *ransomware* o una mula o un monedero alojado por un PSAV situado fuera de la jurisdicción en la que se cometió el ciberataque y que no suele cooperar con las APJs o las UIF.

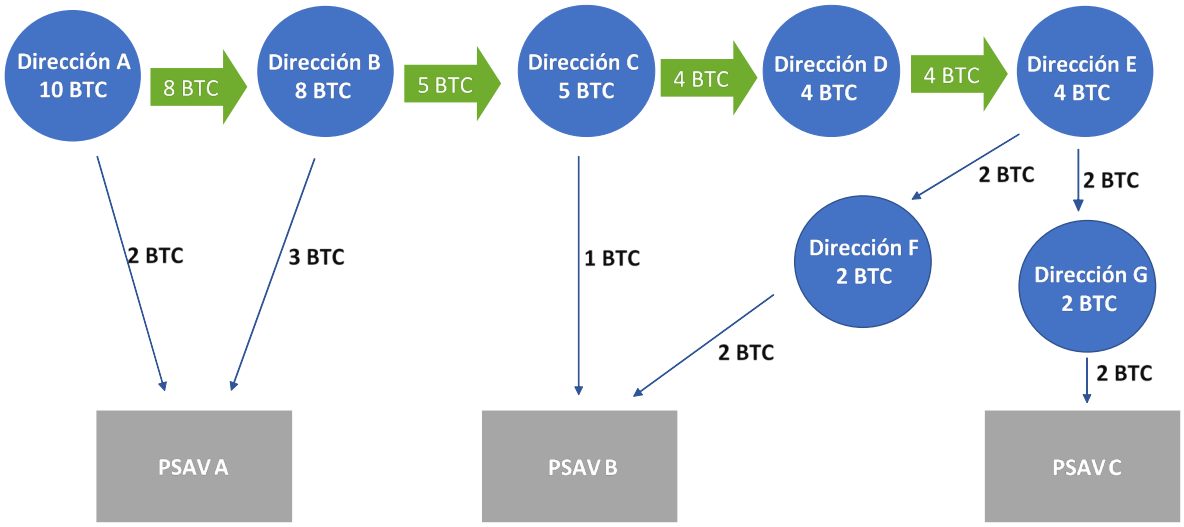
En muchos casos, el delincuente de *ransomware* utiliza diferentes técnicas que suelen facilitar la estratificación (descritas a continuación). Por último, los delincuentes de *ransomware* suelen utilizar a los PSAV situados en jurisdicciones ajenas a la suya para canjear activos virtuales por moneda fiduciaria, aunque también pueden dejar fondos en monederos no alojados durante largos periodos de tiempo o utilizar activos virtuales para pagar a terceros involucrados en los ciberataques.

26. Los delincuentes de *ransomware* suelen utilizar tecnologías, técnicas y *tokens* para reforzar el anonimato en todo el proceso de LD, incluyendo uno o más de los que a continuación se describen. Es posible que los delincuentes de *ransomware* no utilicen siempre los mismos elementos ni sigan el mismo orden al momento de lavar sus ganancias.

    - Los ciberdelincuentes responsables de los ataques de *ransomware* suelen exigir que los pagos de las víctimas en activos virtuales sean enviados a direcciones de monederos que ellos controlan, y a menudo a **direcciones de monederos diferentes** para recibir los ingresos ilícitos de cada ataque.
    - Una vez que los ciberatacantes reciben los fondos, pueden utilizar varias direcciones intermedias para trasladar los activos virtuales de una dirección de monedero, utilizando una serie de transacciones para transferir pequeñas cantidades de activos virtuales a nuevas direcciones de manera sucesiva. A menudo, los fondos se envían a direcciones de monederos alojados en más de un PSAV. Estos patrones de transacción se denominan **cadenas de transacciones**, las cuales no se utilizan exclusivamente para ocultar el movimiento de activos

virtuales.[22] Sin embargo, también pueden ser aprovechados por los ciberdelincuentes para lavar una gran cantidad de activos virtuales a través de una serie de transacciones menores a fin de disminuir la probabilidad de que dicho comportamiento sea rastreado. La ruta de los activos virtuales puede llegar a ocultarse si las transacciones se ejecutan a gran velocidad y de manera frecuente.

Figura 1. Ilustración de una cadena de transacciones



- Los delincuentes de *ransomware* suelen blanquear los activos virtuales a través de **mezcladores o *tumblers*** (por ejemplo, Wasabi), que emplean diversos métodos para ocultar la conexión entre la dirección que envía los activos virtuales y las direcciones que los reciben, ya sea como alternativa o como complemento al movimiento de activos virtuales a través de cadenas de transacciones. En algunos casos, los ciberdelincuentes utilizan transacciones *CoinJoin*, en las que varios remitentes y destinatarios de fondos combinan sus pagos en una única transacción agregada. Esto suele requerir un servicio especializado como *JoinMarket,* que pone en contacto a los usuarios interesados y les ayuda a crear dicha transacción.
- Los ciberatacantes de *ransomware* también utilizan **criptomonedas con anonimato reforzado (AEC; también conocidas como monedas de privacidad)** aunque la mayoría exige el pago en bitcoines. Las experiencias de las jurisdicciones y los informes del sector indican que las AEC son utilizadas para pagar a los ciberatacantes de *ransomware*, ya que pueden ocultar los monederos de envío y recepción. Por ejemplo, las AEC pueden utilizar una combinación de tecnologías de privacidad reforzada, como mezcladores, firmas de círculo, direcciones ocultas y transacciones confidenciales en círculo, que pueden ocultar los monederos de envío y recepción. Cada vez más ciberdelincuentes de *ransomware* solicitan pagos exclusivamente en monero,

[22] Las cadenas de transacciones se observan frecuentemente y pueden ocurrir de forma natural debido a la forma en la que los monederos de activos virtuales están diseñados.

aunque el activo virtual más utilizado en casos de *ransomware* es bitcoin (99%).[23] Algunas jurisdicciones han registrado casos en los que los ciberatacantes aceptaban pagos tanto en bitcoin como en monero. Sin embargo, cobraban una comisión adicional que oscilaba entre 10 y 20% del rescate exigido por los pagos en bitcoines, ya que este tipo de transacciones son más fáciles de rastrear. De este modo, los ciberdelincuentes pagan tasas adicionales por utilizar tecnologías de anonimato reforzado, como los servicios de mezcla, para dificultarle a las autoridades el rastreo o la asignación de transacciones.

- Varias jurisdicciones también señalaron que los ciberdelincuentes suelen convertir el pago del rescate de bitcoines a otros activos virtuales a través de los PSAV o los protocolos DeFi.[24],[25] Esta acción suele denominarse **salto de cadena**, y consiste en pasar de un activo virtual a otra cadena de bloques diferente, a menudo en sucesión rápida y con el propósito de eludir los intentos de rastrear estos movimientos. Una jurisdicción informó que los ciberdelincuentes de *ransomware* utilizan cada vez más los protocolos DeFi para saltar de cadenas a las llamadas criptomonedas estables[26] antes de cambiar los fondos a moneda fiduciaria. Las plataformas DeFi son atractivas para los ciberdelincuentes porque muchas no aplican controles de ALD/CFT, a pesar de que pueden estar sujetas a obligaciones de ALD/CFT en función de los datos y circunstancias de sus modelos de negocio. Una jurisdicción informó del uso sistemático de protocolos DeFi y mezcladores por parte de los ciberdelincuentes de *ransomware*, a veces utilizados repetidamente de manera sucesiva durante el proceso de LD.
- Durante el proceso de LD, los ciberdelincuentes de *ransomware* suelen utilizar los PSAV centralizados, incluyendo operadores extrabursátiles (OTC), para cobrar sus ganancias. Suelen enviar los activos virtuales a un PSAV en jurisdicciones de alto riesgo o a un PSAV con controles ALD/CFT débiles o inexistentes para convertirlos en moneda fiduciaria. Los ciberdelincuentes que radican en jurisdicciones de alto riesgo pueden utilizar los PSAV locales centralizados para estos fines, como el caso de los PSAV situados en Estados Unidos, Suex,[27] Chatex,[28] Garantex[29] y Bitzlato Limited (ver Recuadro 6).[30] Varias jurisdicciones informaron que las instalaciones

---

23 Coveware, *Q3 Ransomware Marketplace Report* (noviembre 2019), disponible en inglés en: www.coveware.com/blog/q3-*ransomware*-marketplace-report.

24 El término finanza descentralizada (DeFi, por sus siglas en inglés) se utiliza cuando aplicaciones descentralizadas o distribuidas, habilitadas por una cadena de bloques con contratos inteligentes ofrecen servicios financieros, como los que ofrecen los PSAV. Una aplicación DeFi (es decir, un programa de software) no es un PSAV según los Estándares del GAFI, ya que estos no aplican ni al software ni a las principales tecnologías. Sin embargo, los creadores, propietarios y operadores u otras personas que ejerzan control o una influencia significativa en los acuerdos DeFi pueden considerarse bajo la definición de GAFI como PSAV si proveen o facilitan activamente servicios de PSAV.

25 Además de utilizarse para lavar los pagos de rescate por *ransomware*, los protocolos DeFi, en particular los puentes entre criptomonedas, se han convertido cada vez más en el objetivo de ciberdelincuentes que tratan de aprovechar las brechas de seguridad y robar activos virtuales.

26 Nota terminológica: El GAFI considera que el término "criptomoneda estable" no es una categoría jurídica o una técnica clara, sino más bien un término de marketing utilizado por los promotores de este tipo de monedas. Para no respaldar involuntariamente dichos argumentos, este informe se refiere a ellas como "las denominadas criptomonedas estables".

27 Comunicado de prensa del Departamento del Tesoro de EE.UU, disponible en inglés en: https://home.treasury.gov/news/press- releases/jy0364

28 Comunicado de prensa del Departamento del Tesoro de EE.UU, disponible en inglés en: https://home.treasury.gov/news/press- releases/jy0471

29 Comunicado de prensa del Departamento del Tesoro de EE.UU, disponible en inglés en: https://home.treasury.gov/news/press- releases/jy0701[30] Comunicado de prensa del Departamento de Justicia de EE.UU., disponible en inglés en: www.justice.gov/opa/pr/founder-and-majority-owner-cryptocurrency-exchange- charged-processing-over-700-million

de cobro están altamente concentradas en zonas urbanas y céntricas. En algunos casos, los ciberdelincuentes de *ransomware* de varios grupos utilizaban los mismos PSAV para recibir o lavar sus activos virtuales.

- En los casos en los que hay varias partes implicadas, los ciberdelincuentes de *ransomware* usualmente pagan a sus socios criminales así como a servidores (*hosts*) de infraestructuras tecnológicas. Los operadores de infraestructuras delictivas están cada vez más dispuestos a aceptar pagos en activos virtuales, y los delincuentes de *ransomware* suelen realizar estos pagos con los ingresos provenientes de sus ciberataques. En numerosos casos, las empresas de análisis de cadenas de bloques han observado desviaciones directas de pagos de rescate por *ransomware* a direcciones de activos virtuales asociadas a operadores delictivos de "infraestructura como servicio" maliciosos.

Recuadro 6. Bitzlato Limited[1]

En enero de 2023, una operación transnacional determinó que Bitzlato Limited, una casa de cambio virtual con un volumen significativo de operaciones en Rusia, desempeñaba un papel fundamental en el lavado de moneda virtual convertible (MVC). La operación fue dirigida por las autoridades francesas y estadounidenses, con el apoyo de Europol y la participación de autoridades de Bélgica, Chipre, Portugal, España y los Países Bajos. Se sospechaba que Bitzlato facilitaba diversas transacciones ilícitas, entre ellas las de ciberdelincuentes de *ransomware*, como Conti, un grupo de RaaS proveniente de Rusia. El Departamento de Justicia de Estados Unidos también indicó que Bitzlato recibió más de 15 millones de dólares en ganancias derivadas de un ataque de *ransomware*. En paralelo, la UIF estadounidense (*Financial Enforcement Network*) emitió una orden en la que identificaba la plataforma como un "problema fundamental de LD".

Estas investigaciones posibilitaron el desmantelamiento de la plataforma de intercambio, incluyendo la incautación de infraestructura digital y activos delictivos por un valor de 18 millones de euros en criptocarteras en Francia, así como la detención de personas clave en varias jurisdicciones.

Bitzlato se promocionaba como una empresa que exigía una identificación mínima a sus usuarios y, como resultado de estos deficientes procedimientos “conozca a su cliente” (CSC), se había convertido en un paraíso para el manejo de ganancias y fondos procedentes de actividades delictivas.

Fuente: Francia y Estados Unidos.

1. Comunicado de prensa de la Gendarmería Nacional Francesa, disponible en francés en: www.gendarmerie.interieur.gouv.fr/gendinfo/enquetes/2023/demantelement-d- une-plateforme-de-cryptomonnaies-servant-au-blanchiment; y Comunicado de prensa de Europol, disponible en inglés en: www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested

27. Algunas jurisdicciones también señalaron que los ciberdelincuentes de *ransomware* utilizaban **mulas de dinero** con cuentas en PSAV para convertir las ganancias nuevamente a moneda fiduciaria mediante el uso de salidas (*off-ramps*) que son servicios/plataformas que permiten el intercambio de activos virtuales por moneda fiduciaria (a veces denominado "cobro" ("*cashing-out*")). Estas cuentas pueden crearse utilizando una identidad falsa o robada o pueden ser cuentas legítimas de otra parte cómplice en el uso de la cuenta. Las mulas de dinero suelen ser terceros no asociados que participan en la fase final del proceso de LD y son responsables de una parte de los fondos globales que fluyen a través de un proceso de LD. Su desvinculación de la entidad delictiva y el hecho de que realizan transferencias de menor valor puede dificultar su identificación.

Recuadro 7. Ejemplo de reclutamiento de mulas de dinero

Los ciberdelincuentes de *ransomware* reclutan mulas de dinero y les proporcionan dispositivos móviles. En la mayoría de los casos, estas no tienen presencia en Internet y sus conocimientos sobre la red son escasos. Las mulas de dinero crean cuentas de correo electrónico con proveedores de servicios de correo electrónico anónimos fuera de las jurisdicciones, lo que dificulta identificar a los usuarios de las cuentas de correo electrónico. Posteriormente utilizan un dispositivo móvil proporcionado por el "gestor" criminal para realizar los procesos de integración y crear una cuenta en la institución financiera o en un PSAV. Una vez incorporados con éxito, las mulas de dinero devuelven el dispositivo al "gestor" criminal. Los "gestores" delictivos utilizan los dispositivos en nombre de la mula de dinero para realizar transacciones en línea. En algunos casos, los ciberdelincuentes se benefician de los servicios de redes privadas virtuales (VPN), que anonimizan la dirección del Protocolo de Internet (IP) del dispositivo utilizado. Como resultado, la ubicación geográfica real del delincuente que realiza las transacciones permanece oculta.

Fuente: Sudáfrica.

SECCIÓN II. RETOS Y BUENAS PRÁCTICAS PARA COMBATIR EL LAVADO DE DINERO PROVENIENTE DEL *RANSOMWARE*

Marco legal

28. Un marco jurídico sólido sirve de base para que las autoridades competentes puedan desarrollar políticas eficaces de mitigación de riesgo de *ransomware*. Esta sección analiza la relevancia de los Estándares del GAFI para (i) criminalizar el *ransomware* vinculado al LD y (ii) adoptar medidas preventivas para los sectores regulados.

El *ransomware* como delito determinante del LD

29. Aunque la mayoría de las jurisdicciones no disponen de legislación penal específica sobre *ransomware*, ello no impide que, en general, persigan penalmente los ataques de *ransomware* como delito determinante.[31]

30. De acuerdo con información de participantes del proyecto, las jurisdicciones tienden a clasificar el delito determinante de *ransomware* como cargos de extorsión o, más comúnmente, como delito informático, daño a datos, intrusión o daño a programas y sistemas informáticos. La Recomendación 3 del GAFI exige que las jurisdicciones penalicen el LD relacionado con delitos de extorsión. Los delitos de extorsión suelen tener la ventaja de ser tecnológicamente neutros, lo que significa que pueden detectar los ataques de *ransomware* independientemente del método o la forma. Las jurisdicciones que utilizan los delitos de extorsión deben asegurarse de que sus leyes sigan manteniendo vigencia para permitir a las autoridades competentes investigar y recuperar eficazmente los flujos de activos virtuales ilícitos (ver sección 6).

31. A diferencia de la extorsión, los delitos informáticos no están incluidos en la lista mínima de delitos determinantes del GAFI.[32] Sin embargo, en la práctica, al parecer esto no ha ocasionado brechas en la persecución de LD derivado de actividades de *ransomware*. Según una muestra de jurisdicciones, las que utilizan la clasificación de ciberdelitos para perseguir el *ransomware* incluyen estos delitos como determinantes (ya sea en la lista designada de delitos determinantes o a través de un "enfoque de referencia a todos los delitos"). Durante la realización del presente estudio, ninguna jurisdicción informó de problemas para perseguir el LD relacionado con *ransomware*. No obstante, las jurisdicciones deben asegurarse de que la elección del delito determinante no inhiba su capacidad para perseguir el LD relacionado con *ransomware*.

Medidas de prevención para agentes relevantes

32. Los Estándares del GAFI exigen a las jurisdicciones aplicar medidas para prevenir el LD, incluso a través de instituciones financieras, las APNFD y los PSAV. Estas medidas garantizan que dichas entidades puedan comprender y mitigar sus riesgos de LD;

---

31 La mayoría de las jurisdicciones informaron que no penalizaban el pago de rescates por parte de las víctimas a los responsables de los ataques de *ransomware*, aunque algunas de ellas desalientan firmemente el pago de rescates por *ransomware* por parte de las víctimas.

32 Ver categorías de delitos definidas en el Glosario de las Recomendaciones del GAFI.

apliquen controles adecuados, incluyendo la identificación de sus clientes, y detecten y denuncien las transacciones sospechosas de conformidad con las Recomendaciones 9 a 23 del GAFI.

33. Dada la relación entre el *ransomware* y los activos virtuales, la modificación realizada en 2018 a los Estándares del GAFI para aplicar estas medidas a los PSAV constituyó un paso importante en la mejora al régimen mundial de ALD/CFT para mitigar los riesgos por *ransomware*. Sin embargo, a enero de 2023[33], de las 86 jurisdicciones evaluadas mediante los Estándares revisados (Recomendación 15), 63 (73%) cumplían con dichas medidas de manera parcial o no las cumplían.[34] Sólo una de las 86 jurisdicciones evaluadas cumplió plenamente con dicha regulación.

34. Dada la diversidad de jurisdicciones evaluadas bajo la Recomendación 15 revisada, es probable que dichas cifras sean muy representativas de la situación actual en toda la red mundial del GAFI. Esta evaluación se encuentra respaldada por los resultados de la encuesta realizada por el GAFI en marzo de 2022, según la cual, en 2022, menos de la mitad de los encuestados disponía de un régimen de concesión de licencias o de registro para activos virtuales y PSAV. Por ello, es probable que en la mayoría de las jurisdicciones existan brechas en la aplicación de obligaciones en materia de ALD/CFT por parte de los PSAV, incluyendo la identificación de clientes o la notificación de operaciones sospechosas. Dada la naturaleza transfronteriza de los activos virtuales, es importante que las jurisdicciones de toda la Red Global aceleren el cumplimiento de la Recomendación 15 (incluyendo la regla de viaje).

Medidas sugeridas

- Las jurisdicciones deben acelerar el cumplimiento de los Estándares del GAFI sobre el sector PSAV mediante la aplicación de la Recomendación 15 (incluyendo la regla de viaje) lo antes posible. Esto garantizará que los PSAV cumplan con las obligaciones necesarias en materia de ALD/CFT para detectar información financiera crítica y denunciar transacciones sospechosas.
- Las jurisdicciones deben garantizar que el *ransomware* se criminalice como delito determinante de LD siguiendo la Recomendación 3 del GAFI (por ejemplo, como tipo de extorsión).

[33] Ver índices de evaluación consolidados, disponibles en inglés en: www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-ratings.html. Es importante considerar que no todas las jurisdicciones han sido evaluadas según la metodología revisada de la Recomendación 15.

[34] El presente análisis se basa en la evaluación mutua y en los informes de seguimiento de las jurisdicciones que han sido evaluadas según la metodología revisada de la Recomendación 15.

Detección y denuncias

35. Debido a la distribución geográfica de los ciberdelincuentes de *ransomware*, a las técnicas de LD utilizadas y a las características actuales de los ataques de *ransomware* (como se ha señalado en la sección I), es difícil estimar la magnitud de los flujos financieros derivados de este fenómeno. En la mayoría de las jurisdicciones, los ataques de *ransomware* siguen sin denunciarse, lo que dificulta establecer un panorama completo de las ganancias financieras y los flujos financieros relacionados con *ransomware*.

36. Una detección y notificación rigurosas sientan las bases para el éxito de investigaciones financieras (ver sección 6). Según la experiencia de las jurisdicciones y los estudios de caso presentados, existen dos fuentes principales para detectar los flujos financieros relacionados con el *ransomware*: los ROS y las denuncias de las víctimas. La siguiente sección explora los retos y las buenas prácticas en relación con el alcance de los requisitos de notificación de los ROS, la identificación de operaciones sospechosas, el fomento de la denuncia por parte de las víctimas, y otras fuentes de detección.

Alcance de las obligaciones de notificación de los ROS

37. Las autoridades competentes suelen utilizar a los ROS para detectar ataques de *ransomware* y como fuente de información durante investigaciones. Al día de hoy, la gran mayoría de los ROS relacionados con pagos de rescate por *ransomware* son presentados tanto por los PSAV como por los bancos.

38. Un pequeño número de jurisdicciones han identificado sectores que no suelen estar sujetos a obligaciones en materia de ALD/CFT como fuentes adicionales potenciales para detectar ingresos ilícitos relacionados con *ransomware*. Incentivar o exigir que estos sectores no tradicionales notifiquen transacciones sospechosas puede ser útil, sobre todo cuando estos participan directamente en la resolución de ataques de *ransomware* en nombre de clientes.

39. Por ejemplo, el sector de seguros, y particularmente las instituciones involucradas en situaciones de *ransomware* y ciberseguros, pueden poseer información directa sobre ataques de *ransomware* que implique a clientes ciber asegurados que hayan presentado solicitudes de reembolso. Estas entidades no están incluidas en la definición de "institución financiera" del GAFI, que incluye la suscripción y colocación de seguros de vida y otros seguros relacionados con inversiones. Sin embargo, a partir de la interacción con dicho sector para promover o solicitar denuncias o informes, algunas jurisdicciones han tenido un impacto positivo inicial respecto a la presentación de denuncias relacionadas con *ransomware*.

Recuadro 8. Divulgación orientada al sector de seguros para mejorar los registros de *ransomware*

En Francia, el sector de seguros distintos al seguro de vida está sujeto a regulación en materia de ALD/CFT. En 2021, se realizaron actividades de acercamiento con este sector a través de grupos de trabajo especializados, que reunieron a representantes del sector público y privado. Dichos grupos de trabajo tenían como objetivo estudiar la posibilidad de asegurar los riesgos cibernéticos y reforzar la resiliencia de las empresas ante ataques cibernéticos. Un producto clave que surgió de dichos grupos de trabajo fue un informe publicado[1] que incluye, entre otros, la evolución del riesgo de LD relacionado con el *ransomware*, así como las obligaciones en materia de ALD/CFT y las buenas prácticas relacionadas con el pago y el reembolso de los rescates.

Adicionalmente, la Autoridad de Supervisión Prudencial y de Resolución (ACPR, por sus siglas en francés) realizó una supervisión específica a las compañías de seguros, incluso durante inspecciones presenciales. Posteriormente, la ACPR recordó a las entidades reguladas sus requerimientos en materia de ALD/CFT al momento de contratar dichos servicios, incluyendo la necesidad de controlar y obtener cualquier información financiera relevante (especialmente para el rastreo de pagos).

Desde entonces, TRACFIN ha observado un aumento en los ROS vinculados a pagos por *ransomware* registrados por el sector de seguros, de 28 en 2020 y 19 en 2019, a 66 en 2021. El incremento en 2021 se atribuye en parte solo a una compañía de seguros y los volúmenes aún no son lo suficientemente significativos como para establecer conclusiones o resultados.

Fuente: Francia.

1. Disponible en francés en www.banque-france.fr/sites/default/files/rapport_45_f.pdf

40. Las empresas de respuesta a incidentes también tienen acceso a información oportuna relacionada con ataques de *ransomware* y de pagos. Estas empresas, como las de respuesta a incidentes forenses digitales y firmas legales, ayudan a las víctimas de ataques de *ransomware*, facilitando los pagos a los cibercriminales negociando los montos de pago, convirtiendo la moneda fiduciaria del cliente en activos virtuales, y transfiriendo los fondos a cuentas controladas por los ciberdelincuentes. El fomentar o requerir la presentación de informes a este sector permite detectar y denunciar oportunamente los ataques de ransomware, sobre todo porque es probable que los clientes, en primera instancia, informen a estas entidades del ataque (en algunos casos incluso antes de que lo hagan ante las APJs). Dependiendo del modelo de negocio y de los servicios que proveen, estas empresas pueden clasificarse bajo la definición de PSAV (y consecuentemente estar sujetas a obligaciones de registro de ALD/CFT y de ROS) si operan como negocio para o en nombre de otra persona física o moral, si intercambian activos virtuales por otros activos virtuales o por moneda fiduciaria, o si transfieren, custodian o administran activos virtuales.

Recuadro 9. Regulación de empresas de análisis forense digital y de respuesta a incidentes

Las empresas de análisis forense y de respuesta a incidentes (DFIR, por sus siglas en inglés) y las compañías de ciberseguros (CICs, por sus siglas en inglés) pueden ayudar a las víctimas de ataques de *ransomware* prestando servicios para facilitar los pagos de *ransomware*. En 2020 y 2021, FinCEN (la UIF de Estados Unidos) aclaró en varios avisos sobre *ransomware*[1] que, dependiendo de los hechos y las circunstancias, esta actividad podía considerarse como una transmisión de dinero. Las entidades transmisoras de dinero deben registrarse como empresas de servicios monetarios y están sujetas a las obligaciones en materia de ALD/CFT. Los avisos también incluían indicadores financieros de alerta o de *ransomware* y pagos asociados a este para que las DFIRs y las CICs ayuden a identificar actividades sospechosas y registren los reportes de operaciones sospechosas (ROS).

Durante el primer semestre de 2021, las denuncias presentadas por empresas DFIR con sede en Estados Unidos representaron aproximadamente 63% de los ROS relacionados con *ransomware*[2]. El número total de denuncias relacionadas con *ransomware* recibidas por la FinCEN en 2021 también aumentó en 188%. Estos registros permitieron al FinCEN analizar y descubrir información sobre patrones y tendencias para redoblar los esfuerzos del gobierno para prevenir y combatir los ataques de *ransomware*. Por ejemplo, el análisis del FinCEN reveló que en 2021 el *ransomware* sigue representando una amenaza significativa para los sectores de infraestructuras críticas de Estados Unidos, así como para las empresas y el público en general. El análisis destacó que las variantes de *ransomware* relacionadas con Rusia constituyen la mayor parte de la actividad de *ransomware* reportada, representando 69% del valor de incidentes de *ransomware* y 75% de los incidentes relacionados con *ransomware* en la segunda mitad de 2021[3].

Fuente: Estados Unidos.

Notas

1. Disponible en francés en www.banque-france.fr/sites/default/files/rapport_45_f.pdf
2. Ver *FinCEN's Financial Trend Analysis*, disponible en: www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf
3. Ver *FinCEN's Financial Trend Analysis*, disponible en: www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf

41. Lo anterior muestra la utilidad de alentar o requerir la presentación de denuncias a una amplia gama de sujetos obligados no tradicionales, en función del riesgo y del contexto. Esto permite que actividades sospechosas sean reportadas y registradas desde la perspectiva de diversos sectores, mejorando las habilidades de las autoridades para descubrir y detectar incidentes en cualquier sector.

Medidas para mejorar la detección de transacciones sospechosas

42. Las jurisdicciones reconocen que por lo general los sectores no denuncian todas las actividades sospechosas relacionadas con *ransomware*. Pueden existir retos de detección debido a la naturaleza geográficamente descentralizada de los grupos criminales de *ransomware*, la variedad de delincuentes involucrados, y el uso de diferentes técnicas de LD. Es muy probable que ningún sector tenga una perspectiva completa de dicha problemática.

43. Para mejorar la frecuencia y calidad de la presentación de reportes por parte de los sujetos obligados y lograr una mayor detección de incidentes, las jurisdicciones han recurrido a diversos métodos como involucrar al sector privado, así como desarrollar e intercambiar indicadores de alerta y guías de detección (ver sección 8.3).

Recuadro 10. Documento de orientación sobre *ransomware* de la Autoridad para la Prohibición de Lavado de Dinero y la Financiación del Terrorismo de Israel (IMPA, por sus siglas en inglés)

El IMPA, la UIF de Israel, realizó un análisis estratégico de los informes de actividades inusuales para identificar las características de los pagos por *ransomware*. Dicho análisis incluyó información sobre la frecuencia y el tipo de entidades sujetas a ataques, los montos pagados, el tipo de activos virtuales utilizados y la participación de terceros. El análisis derivó en la publicación de un documento de orientación sobre *ransomware* que incluía alertas y estudios de caso. El documento se envió a todos los sujetos obligados pertinentes y se publicó en el sitio web del IMPA[1] junto con un comunicado de prensa oficial.

Los resultados de la investigación se presentaron en foros públicos y conferencias profesionales. La publicación promovió, entre varios temas, el acercamiento con el sector de respuesta a incidentes israelí, para continuar profundizando dichas relaciones y explorar oportunidades de cooperación e intercambio de información en el futuro.

Fuente: Israel.

1. Sólo disponible en hebreo en: www.gov.il/BlobFolder/dynamiccollectorresultitem/red-flags-typology-ransomware-impa-140222/he/professional-docs_red_flags_typology_ransomware_impa_140222.pdf

44. En la mayoría de los casos en los que un PSAV realiza un ROS relacionado con *ransomware*, este se clasifica con base en la sospecha de que se han comprado activos virtuales para pagar una demanda de rescate. Los indicadores útiles en los que los PSAV se basan incluyen las declaraciones de las víctimas a los PSAV, las compras de dichos activos realizadas por una empresa de respuesta a incidentes conocida, así como los pagos realizados vinculados directa o indirectamente a la dirección de un activo virtual con exposición al *ransomware* identificado a través del análisis de cadena de bloques. Dado que los PSAV actúan como intermediarios directos en muchos pagos de rescate, son una fuente clave de ROS sobre flujos financieros ilícitos relacionados con *ransomware*. Para una recopilación de los indicadores de riesgo relevantes utilizados por los PSAV, consultar el informe del GAFI *Countering Ransomware Financing: Potential Risk Indicators* (disponible en inglés).

Recuadro 11. Participación de una empresa de gestión de crisis

El IMPA recibió un ROS a través de un PSAV israelí relativo a una empresa de gestión de crisis (respuesta a incidentes) que compró activos virtuales (valuados en decenas de miles de dólares de ese momento) para pagar un ataque de *ransomware* en nombre de una víctima no revelada. Según el ROS, una cantidad adicional en criptomonedas fue adquirida de manera independiente por un representante del presunto destinatario del ataque desde el mismo PSAV israelí.

La investigación financiera del IMPA reveló que la dirección del monedero que recibió la mayor parte de los fondos estaba relacionada con otros ataques de *ransomware* y recibía fondos de otras direcciones. Los fondos acumulados se transfirieron posteriormente a un PSAV situado en una jurisdicción de alto riesgo. Los fondos que fueron adquiridos de manera independiente por la empresa se transfirieron a través de varias direcciones, y gran parte de ellos se canalizaron a través de un mezclador. Posteriormente se envió un informe de inteligencia a las APJs para que continuaran con la investigación.

Fuente: Israel.

45. A diferencia de los PSAV, los bancos y otras instituciones financieras y de pago pueden percatarse de que una víctima está transfiriendo moneda fiduciaria a un PSAV o a un tercero que actúa en nombre de la víctima relacionada con un pago de rescate y con ello pueden registrar el correspondiente ROS. Sin embargo, posiblemente no cuenten con información directa sobre los pagos relacionados con el *ransomware* o el LD asociado a este, ya que la mayoría de los pagos se realizan en activos virtuales y no en moneda fiduciaria. Como resultado, estas instituciones financieras y de pago cuentan con información muy limitada sobre las direcciones de los activos virtuales o el origen de los fondos, dificultándoles realizar el análisis de cadenas de bloques. Para afrontar más ágilmente los retos antes mencionados, en muchos casos dichas instituciones requieren de indicadores indirectos para identificar posibles pagos de *ransomware*. Según estudios de caso, los indicadores comunes incluyen transferencias inusuales a los PSAV (especialmente cuando la empresa no suele operar con activos virtuales), la compra de activos virtuales por parte de empresas de ciberseguridad, de seguros y de respuesta a incidentes, las propias declaraciones de los clientes de que se está utilizando una transferencia bancaria para pagar una demanda de rescate, así como información de fuentes abiertas que corroboren el ciberataque (por ejemplo, comunicados de prensa, informes de incidentes, etc.). Para una lista detallada de indicadores de riesgo relevantes, consultar el documento del GAFI *Countering Ransomware Financing: Potential Risk Indicators* (disponible en inglés).

Denuncia de víctimas

46. Debido a los bajos niveles de denuncia de transacciones sospechosas sobre pagos de *ransomware* en la mayoría de las jurisdicciones, los ROS siguen siendo una fuente insuficiente para detectar o comprender el alcance completo de los ataques de *ransomware* y el LD relacionado a este y como elemento para apoyar las investigaciones. Es por ello que las denuncias de las víctimas constituyen una fuente importante de información para detectar e investigar los flujos financieros relacionados con el *ransomware*. La denuncia oportuna por parte de las víctimas es importante para que las APJs puedan actuar con rapidez, rastrear los flujos financieros, y aumentar las probabilidades de éxito de procuración de justicia.

47. Los requisitos de denuncia de incidentes varían según la jurisdicción y dependen del marco jurídico de cada una de ellas. En la mayoría de los casos, la denuncia de incidentes es voluntaria. Cuando las víctimas denuncian, suelen hacerlo ante la policía, las agencias de ciberseguridad, las unidades especiales de denuncia de ciber-incidentes o ante los equipos de respuesta a emergencias informáticas (EREI) locales.

48. Sin embargo, se ha observado que las denuncias de las víctimas son limitadas, puesto que los ataques no se denuncian plenamente. Hay varias razones que pueden desalentar a las víctimas a denunciar voluntariamente los ataques de *ransomware* relacionadas con la percepción de posibles conflictos contra sus propios intereses empresariales. Esto incluye la preocupación sobre daño reputacional, el deseo de restablecer rápidamente las operaciones o el miedo a represalias por parte de los ciberdelincuentes. La naturaleza del *ransomware* suele implicar el acceso ilícito a datos personales y confidenciales de los clientes. Admitir fallas de seguridad o datos ante las APJs o ante el público se percibe como algo que afecta negativamente a las empresas y puede dar lugar a demandas civiles. Las víctimas también pueden sentirse amenazadas por filtraciones públicas de datos por parte de los ciberdelincuentes si se notifica a las APJs.

49. Además, las víctimas pueden no tener incentivos para denunciar voluntariamente los incidentes tras el pago del rescate. En los casos en que las víctimas disponen de un ciberseguro, es posible que carezcan de motivación financiera para denunciar un ataque, ya que la compañía de seguros puede cubrir el costo del rescate. En algunas jurisdicciones, es posible que las víctimas no denuncien el pago de rescates por temor a infringir la regulación nacional (por ejemplo, los pagos efectuados a una entidad sancionada) o a ser consideradas cómplices de los grupos delictivos.

50. Las jurisdicciones han adoptado una serie de métodos para alentar a las víctimas a denunciar los ataques de *ransomware*. Por ejemplo, algunas jurisdicciones han implementado políticas o realizado actividades como campañas públicas para sensibilizar sobre dichos ataques y promover su denuncia. Estas políticas y actividades suelen igualmente involucrar al sector privado y sirven para enfatizar cómo las autoridades pueden ayudar a mitigar el impacto de los ataques de *ransomware*. Esto incluye devolver los activos a las víctimas y compartir claves de desencriptado para, en la medida de lo posible, recuperar datos.

Recuadro 12. No Más Rescates[1]

El sitio web "*No More Ransom*" ("No Más Rescates") es una iniciativa de la Unidad Nacional de Delincuencia de Alta Tecnología de la policía de los Países Bajos, el Centro Europeo de Ciberdelincuencia de Europol y dos socios del sector, cuyo objetivo es ayudar a víctimas de *ransomware* a recuperar sus datos cifrados sin tener que pagar a los ciberdelincuentes. El sitio web contiene un repositorio de claves y aplicaciones que pueden desencriptar datos bloqueados por distintos tipos de *ransomware*. Esto ayuda a las víctimas a recuperar el acceso a sus archivos cifrados o a sus sistemas bloqueados sin tener que pagar el rescate.

La iniciativa reúne a numerosos socios de los sectores público y privado en diversas jurisdicciones, incluyendo APJs y empresas de seguridad informática. Su objetivo es orientar a los usuarios sobre el funcionamiento del *ransomware* y las contramedidas que pueden tomarse para prevenir eficazmente la infección una vez realizado el ataque. El sitio web promueve que las víctimas no paguen ningún rescate y proporciona enlaces para redirigirlas al sitio web de denuncia de sus países para presentar una denuncia formal del incidente.

Fuente: *No More Ransom*.

1. Para mayor información, consultar www.nomoreransom.org/en/index.html

51. Para mitigar las preocupaciones por el riesgo reputacional asociado a denuncias, algunas jurisdicciones han intentado crear espacios seguros para que las empresas víctimas de ataques de *ransomware* se pronuncien sin temor al daño reputacional, por ejemplo, mediante encuentros periódicos y la asistencia a conferencias empresariales. Otra buena práctica es la creación de sitios web de ventanilla única que sirven como un espacio único para que las víctimas denuncien incidentes al igual que como centro de asesoramiento de expertos y de acciones correctivas. Aunque estos esfuerzos suelen centrarse en detectar los ataques de *ransomware,* la información obtenida de la denuncia de la víctima es vital para las investigaciones financieras, incluyendo el rastreo de los flujos financieros y el LD asociado.

Recuadro 13. Centro Canadiense de Ciberseguridad

El Centro Canadiense de Ciberseguridad (Centro Cibernético) se inauguró en 2018 como una iniciativa clave en el marco de la Estrategia Nacional de Ciberseguridad de Canadá. Constituye una fuente unificada de asesoramiento experto, orientación, servicios y apoyo en materia de ciberseguridad para el gobierno, los propietarios y operaciones de infraestructuras críticas, el sector privado, y el público canadiense. Ofrece recursos a particulares y empresas, incluyendo orientación sobre cómo prevenir y recuperarse de incidentes de *ransomware,* y presenta informes sobre el panorama de amenazas de *ransomware*. El Centro Cibernético recopila denuncias de incidentes cibernéticos de las partes interesadas de los sectores público y privado, tanto nacionales como internacionales. Las denuncias pueden realizarse en línea, por correo electrónico o vía telefónica. El Centro recomienda informar a la policía si se cree que un incidente cibernético representa una amenaza inminente para la vida o si es de naturaleza delictiva.

Fuente: Canadá.

52. Algunas jurisdicciones han adoptado el enfoque de identificar determinadas industrias o instancias en las que la denuncia por parte de la víctima es obligatoria, por ejemplo, en el caso de ataques a infraestructuras críticas (como sectores de energía, comunicaciones, sanidad, etc.) o en caso de filtración de datos. En muchas jurisdicciones, estas industrias también pueden incluir sectores financieros sujetos a obligaciones de ALD/CFT (por ejemplo, la banca), donde las entidades reguladas están obligadas a denunciar incidentes relevantes a las autoridades competentes, tales como los supervisores, como parte del marco regulatorio. Los mecanismos de protección de datos también pueden promover o requerir la presentación obligatoria de denuncias por violación de datos personales, lo que puede facilitar la detección oportuna. Para mejorar la detección de flujos financieros ilícitos, una buena práctica es capturar la información financiera relevante durante cualquier denuncia (como la dirección del monedero o el tipo de activo virtual).

Otras fuentes de detección

53. Como se indicó anteriormente, los intercambios y la colaboración con partes interesadas ajenas a las instituciones financieras, las APNFD y los PSAV, tales como los proveedores de servicios de Internet y el sector de ciberseguridad, constituyen una fuente valiosa y potencial de información. Sin embargo, dichos sectores pueden no estar sujetos a regulación en materia de ALD/CFT, incluyendo la presentación de ROS. En algunos casos, pudiera existir un posible conflicto de intereses (por ejemplo, las empresas de ciberseguridad que actúan en nombre de las víctimas) que limite la presentación proactiva de denuncias. Ante tales circunstancias, la información pudiera obtenerse a través de mecanismos informales, ya sea a través de colaboraciones público-privadas en las estas entidades participen o mediante una intervención directa.

Recuadro 14. Colaboración con una empresa de ciberseguridad

Una compañía afectada contrató a una empresa de ciberseguridad tras sufrir un ataque de un grupo de *ransomware* en donde el rescate se exigió en bitcoines o en monero. La víctima pagó el rescate al grupo delictivo a través de la empresa de ciberseguridad.

Posteriormente, la empresa de ciberseguridad informó a las APJs del incidente, lo que les permitió rastrear los flujos ilícitos. La autoridad colabora frecuentemente con empresas de ciberseguridad. Esta colaboración pretende interferir lo menos posible en el trabajo de recuperación que las empresas de ciberseguridad realizan para sus clientes, pero garantizando que se proporcionen elementos clave como direcciones IP y criptográficas para las investigaciones penales.

En este caso, las APJs observaron el uso de técnicas de anonimato como el uso de mezcladores, así como de numerosas direcciones de billeteras no alojadas. En el momento de la investigación, una parte significativa de los activos se guardaba en billeteras no alojadas, por lo que fue imposible rastrearlos. Se reportó que una parte considerable de los fondos se había canalizado a través de dos PSAV en jurisdicciones extranjeras.

Fuente: Suiza.

54. Las autoridades competentes también han detectado ataques y pagos de *ransomware* a través de investigaciones financieras independientes utilizando el análisis de cadenas de bloques en monederos conocidos por estar vinculados con el *ransomware*. Esto incluye el seguimiento de ataques conocidos, blogs y análisis de código abierto compartidos por empresas de análisis de cadenas de bloques, así como el contacto proactivo con víctimas potenciales tras el análisis.

55. Estos esfuerzos pueden revelar pistas adicionales sobre ataques previos de *ransomware*. También pueden revelar información sobre la magnitud de un ataque atribuible a un delincuente de *ransomware*, así como las tendencias, tipologías e infraestructuras utilizadas por los ciberdelincuentes para lavar, recibir y utilizar los fondos provenientes de sus ganancias ilícitas.

Recuadro 15. Análisis de fuentes abiertas para identificar a los delincuentes de RaaS

La UIF de Turquía recibió el ROS de un PSAV referente a una dirección de monedero vinculada a una persona registrada por dicho PSAV como "Nombre 1". Una búsqueda en línea del nombre reveló que existe un sitio web con el mismo nombre. Las investigaciones posteriores demostraron que el sitio web realizaba actividades relacionadas con la *dark web* y servía de intermediario en la venta de programas de *ransomware* y otros softwares maliciosos.

Un análisis más detallado basado en fuentes abiertas reveló que:

- La persona implicada en la transacción mencionada en el ROS utilizaba un apodo diferente ("Nombre 2"). Esto condujo a la identificación del nombre real del sospechoso ("Persona X"). Este anteriormente ya era considerado una persona de interés por la Oficina de Lucha contra el Cibercrimen del Departamento de Policía.
- El sospechoso ("Persona X") ofrecía servicios y productos como accesos no autorizados, acceso a información confidencial, credenciales de identidad falsas, ciberataques a cuentas de redes sociales, venta de enlaces maliciosos (*hacklinks*) y páginas de *phishing*.
- Los pagos por estos productos/servicios ilegales se realizaban en bitcoines y otros activos virtuales.

Posteriormente, la UIF de Turquía solicitó al PSAV información adicional relacionada con la persona incluida en el ROS, especialmente direcciones de monederos, transacciones financieras (tanto de activos virtuales como de moneda fiduciaria) y más información personal. Se preparó un informe analítico y se presentó a los Departamentos de Ciberdelincuencia de la Policía Nacional turca, bajo la sospecha de que la persona incluida en el ROS era un intermediario en la venta de *ransomware* y otros programas maliciosos. Las investigaciones continúan al día de hoy.

Fuente: Turquía.

56. Las jurisdicciones pueden igualmente ser alertadas de ataques y pagos de *ransomware* a través de información compartida por otras jurisdicciones. La cooperación internacional, la asistencia jurídica mutua y el intercambio informal de información con jurisdicciones extranjeras pueden proporcionar información sobre los fondos captados a través de intercambios nacionales vinculados a ataques/víctimas extranjeras.

Acciones propuestas

- Las jurisdicciones deben apoyar a los sujetos obligados a detectar el *ransomware* y el LD relacionado con este, así como a denunciar transacciones sospechosas, compartiendo tendencias, guías de detección e indicadores de alerta (como los incluidos en el documento del GAFI *Countering Ransomware Financing: Potential Risk Indicators,* disponible en inglés) con los sujetos obligados relevantes.
- Las jurisdicciones deben incentivar a las víctimas a denunciar voluntariamente los incidentes, por ejemplo, informándoles sobre los apoyos y recursos disponibles o estableciendo canales seguros para presentar denuncias.
- Las jurisdicciones deben considerar la posibilidad de establecer canales de comunicación con actores no tradicionales que pudieran no estar sujetos a las obligaciones de ALD/CFT (como las compañías de ciberseguros y de respuesta a incidentes) para aumentar las fuentes de detección.

Estrategias de investigación financiera

57. El objetivo de casi todos los ataques de *ransomware* es generar ganancias. La mayoría de las jurisdicciones reconocen que las investigaciones de *ransomware* tienen un componente financiero importante. Los estudios de caso muestran que el rastreo de activos virtuales es una parte fundamental de las investigaciones de *ransomware*. En las jurisdicciones que informaron sobre la investigación de ataques de *ransomware*, suele haber una investigación financiera paralela que rastrea el pago del rescate.

58. A nivel mundial, se observa una evidente falta de experiencia en las investigaciones de LD relacionadas con *ransomware*. Muy pocas jurisdicciones han presentado cargos de LD asociados con *ransomware*. Esto puede atribuirse, en parte, a los retos que implica la detección y denuncia, como se discutió anteriormente en la sección 5.

59. Dicha sección explora los retos específicos y las buenas prácticas en investigaciones financieras sobre *ransomware* y LD relacionado a este que han sido exitosas, incluyendo (i) el trabajo realizado con las víctimas para acceder a información; (ii) las técnicas y mecanismos de investigación; y (iii) la recuperación de activos.

Actuar con rapidez y colaborar con las víctimas para acceder a información

60. Dada la naturaleza de ciberdelitos como el *ransomware*, los resultados exitosos de procuración de justicia dependen de la capacidad de actuar con rapidez y recopilar información clave relacionada con el ataque de *ransomware* y su pago. Lo anterior incluye detectar las direcciones de los activos virtuales, el importe total del rescate y el tipo de activo virtual utilizado, las fechas de las transferencias, los tipos de servicios involucrados, la identidad de la víctima, las comunicaciones entre la víctima y los delincuentes de *ransomware*, así como cualquier tercero implicado en el pago del rescate.

61. En muchos casos, la recopilación de dicha información depende de la cooperación de las víctimas o de terceros involucrados en la respuesta al incidente y/o en el proceso de pago del rescate. Sin embargo, como ya se ha comentado, las víctimas pueden

mostrarse reacias a informar sobre los incidentes a las APJs (ver sección 5.3). Las víctimas pueden igualmente negarse a cooperar debido a la percepción de intereses contrapuestos con las APJs ya que, a menudo, las víctimas desean reanudar sus operaciones comerciales lo antes posible y pueden llegar a preferir pagar el rescate. También pueden temer a represalias por parte de los ciberdelincuentes por involucrar a las APJs. Por otra parte, las APJs pueden requerir de tiempo para obtener pruebas forenses, desarrollar operaciones controladas y realizar otras medidas de investigación, lo que puede retrasar la reactivación de los servicios.

62. Las denuncias tardías o incompletas, así como la falta de cooperación por parte de las víctimas, pueden comprometer la calidad de la información disponible para proseguir con éxito y profundizar en las investigaciones. La ausencia de un plan de acción claro para que las víctimas realicen acciones posteriores al ataque y/o el pago puede comprometer las pruebas disponibles debido a la falta de preservación de datos. Las buenas prácticas abordadas en la sección 5.3, tales como las campañas públicas y otros esfuerzos para promover la participación de las víctimas, son fundamentales para aminorar estos retos.

63. Algunas jurisdicciones destacaron la importancia de compartir información entre investigadores cibernéticos (predicados) e investigadores de LD. Durante la recopilación de pruebas forenses para la investigación determinante de cualquier *ransomware*, las APJs inevitablemente recopilarán información relevante para investigar el LD asociado. Dicha información permite a las APJs establecer conexiones entre los diferentes grupos y entes afiliados de los atacantes de *ransomware*, y proporcionar pistas de seguimiento para realizar una investigación financiera más amplia (para mayor información sobre esquemas de cooperación eficaz entre distintas autoridades nacionales competentes, ver sección 8.2).

Recuadro 16. Fuentes relevantes de evidencia para investigaciones financieras obtenidas durante el proceso de realización de investigaciones determinantes

Pruebas forenses. Ejemplos de estas incluyen: vectores de ataque (es decir, cómo los delincuentes logran obtener accesos no autorizados); información sobre la variante de *ransomware*; direcciones IP; nombres o alias utilizados; y dispositivos del atacante. Dicha información puede obtenerse directamente de las víctimas, los proveedores de servicios de Internet, las empresas de ciberseguridad y de respuesta a incidentes, así como mediante el uso de tecnología forense.

Pruebas directas del sector privado. Entre las empresas relevantes del sector privado se encuentran las propietarias de la tecnología o infraestructura que se utilizó indebidamente en el ataque de *ransomware*. Los investigadores pueden obtener información sobre los suscriptores de las empresas de correo electrónico o de redes sociales en las que el agresor pudiera haber tenido cuentas para comunicarse con la víctima.

Información de fuentes abiertas: la revisión de información de fuentes abiertas, incluyendo redes sociales, foros en línea, mercados en la *dark web* y comunicaciones realizadas por delincuentes de *ransomware*, puede ayudar a identificar a posibles perpetradores de ataques de *ransomware*.

Técnicas y mecanismos de investigación

Relevancia de las técnicas de investigación tradicionales

64. Las tecnologías utilizadas por los ciberdelincuentes de *ransomware* para ocultar sus ubicaciones, identidades y flujos financieros pueden dificultar las investigaciones. Entre los retos particulares está el uso de VPN, "el enrutamiento por capas" [35] o el correo electrónico cifrado para permitir una mayor privacidad y seguridad, y una actividad anónima a medida que el tráfico se desplaza por la red. Estos retos pueden complicarse aún más debido a la rapidez con la que evolucionan dichas tecnologías.

65. La Recomendación 31 del GAFI sienta las bases para dotar a las APJs de las competencias necesarias para llevar a cabo investigaciones financieras efectivas. Dichas técnicas de investigación tradicionales siguen siendo importantes para superar estos retos y permitir la recopilación y el análisis de información clave relacionada con flujos financieros asociados al *ransomware*. Lo anterior incluye la vigilancia, intercepción de comunicaciones, así como operaciones encubiertas. Sin embargo, dichas técnicas tradicionales deben adaptarse al contexto en el que se realizan las investigaciones financieras relacionadas con activos virtuales. Entre los ejemplos de cómo lograr resultados satisfactorios en la investigación figuran los siguientes:

- *Vigilancia*: determinar los tipos de dispositivos electrónicos utilizados por el sospechoso; detectar cualquier monedero utilizado, así como sus métodos preferidos de comunicación electrónica.
- *Intercepción de comunicaciones y operaciones encubiertas*: adquirir conocimientos sobre las actividades del sujeto y el funcionamiento de una organización delictiva, identificando a las personas asociadas con el sujeto e información financiera y activos relevantes, así como infiltrarse en comunidades delictivas (como los foros de la *dark web*) para retirarle el anonimato a los perpetradores del delito y beneficiarios finales.
- *Órdenes de producción*: obtención de información de los PSAV u otras instituciones financieras implicadas en el pago de rescates, etc.

66. El uso de estas herramientas en investigaciones financieras puede fortalecerse por los datos obtenidos a través de los ROS o por las denuncias de las víctimas (ver sección 5). Las APJs pueden identificar las instituciones financieras relevantes y los PSAV a través de ROS y análisis de cadenas de bloques (ver sección 6.2.2), para obtener las pruebas necesarias a través de órdenes de producción. Los PSAV pueden proporcionar información útil para que las investigaciones financieras relacionadas con *ransomware* puedan obtener información básica y útil sobre la propiedad y las transacciones (por ejemplo, la identidad del usuario e información relacionada, direcciones IP, tarjetas de crédito o cuentas bancarias, etc.).

67. Sin embargo, como se indica en la sección 3, algunas redes de *ransomware* también se han vinculado a jurisdicciones de alto riesgo en las que los requisitos en materia de ALD/CFT para los PSAV son débiles o inexistentes, o en las que los PSAV suelen incumplirlos. Por lo tanto, las investigaciones pueden verse afectadas si los fondos se mueven a través de estos PSAV o son retenidos por ellos. En tales casos, es posible que los PSAV no recopilen ninguna información relevante o no respondan a solicitudes de las APJs.

---

[35] También conocido por sus siglas como “TOR”, es un software de código abierto que permite a los usuarios navegar por Internet de forma anónima.

68. Los investigadores se enfrentan a retos similares cuando los delincuentes utilizan billeteras no alojadas, ya que esto proporciona a los usuarios el control de activos virtuales sin la participación de un PSAV. Lo anterior plantea retos para detectar y prevenir la actividad de LD. La falta de una conexión con una tercera entidad (que debería estar registrada/licenciada según los Estándares del GAFI) puede complicar la capacidad de las autoridades para identificar al propietario del monedero, ya que no hay una entidad externa de la cual se pueda recabar información.

69. La implementación limitada de la "regla de viaje" del GAFI por parte de los PSAV igualmente ofrece a los ciberdelincuentes la oportunidad de evitar ser detectados y obstaculizar las investigaciones. La regla de viaje establece que los PSAV y otras instituciones financieras que participen en transferencias de activos virtuales compartan información sobre el remitente (originador) y el destinatario (beneficiario) junto con cualquier transferencia. Esto aumenta la transparencia de las transacciones para prevenir abusos delictivos y es una fuente de información a la que las APJs pueden acceder para identificar a las partes implicadas en una transacción determinada. Sin embargo, un informe del GAFI de 2022 reveló que sólo un tercio de las jurisdicciones declaran haber promulgado legislación para aplicar la regla de viaje a los PSAV, e incluso una proporción menor no ha aplicado realmente estos requisitos.[36] Esta falta de regulación consistente reduce la cantidad de información disponible para las APJs procedente de los PSAV en jurisdicciones que no están sujetas a la regla de viaje. También significa que los PSAV de jurisdicciones que cumplen con la regulación y realizan transacciones con PSAV de jurisdicciones que no la cumplen probablemente no puedan obtener información, limitando la información disponible para los investigadores incluso en jurisdicciones que se apegan a la regla de viaje.

36 GAFI (junio 2022) *Targeted Update on Implementation of the FATF Standards on Virtual Assets And Virtual Asset Service Providers*. Este documento sólo incluye a países cuyos MERs/FUR se publicaron a partir de junio de 2021 y mayo de 2022.

Recuadro 17. Técnicas de investigación tradicionales y financieras contra un grupo de *ransomware*

Una empresa víctima italiana presentó una denuncia policial tras efectuar el pago de rescate en bitcoines y desbloquear con éxito sus datos infectados por un ataque de *ransomware*. El pago se realizó a través de un PSAV mencionado en la solicitud de rescate.

Las investigaciones policiales contra el PSAV descubrieron que su sitio web estaba registrado formalmente en Italia. Más tarde, se identificó a un sujeto italiano y se descubrió que había facilitado los flujos de bitcoines vinculados al pago del rescate. Posteriormente, la policía registró su apartamento y aseguró tarjetas de pago, teléfonos móviles, así como artículos de hardware como discos duros, unidades USB y tabletas móviles. Las intervenciones telefónicas y el análisis de los mensajes de telefonía móvil intercambiados permitieron identificar a un grupo de otros sujetos italianos (el "Grupo") que desempeñaban papeles similares en la facilitación de flujos de bitcoines relacionados con el *ransomware*. Investigaciones financieras descubrieron que los fondos fiduciarios enviados por las víctimas del *ransomware* fueron transferidos por el Grupo a cuentas bancarias extranjeras mantenidas por PSAV extranjeros, incluyendo aquellos ubicados en jurisdicciones de alto riesgo.

Con base en las investigaciones financieras, así como en el análisis forense de los teléfonos y los componentes del hardware, las autoridades concluyeron que el Grupo estaba propagando el *ransomware* a las víctimas, con importes de rescate de varios cientos de euros por cada ataque. El Grupo ha sido acusado de extorsión relacionada con *ransomware* y posterior lavado de los ingresos, que se estimaron en un total de aproximadamente €300 000 obtenido de varias víctimas. Las investigaciones siguen en curso.

Fuente: Italia.

Técnicas específicas de activos virtuales

70. Además de las técnicas tradicionales, las APJs deben utilizar técnicas específicas de activos virtuales para llevar a cabo investigaciones financieras relacionadas con *ransomware*. La mayoría de los activos virtuales operan en una cadena de bloques pública que actúa como una base de datos visible a través de la cual puede rastrearse la información seudónima asociada a las transacciones de activos virtuales, utilizando herramientas de análisis de cadenas de bloques de código abierto o de suscripción (ver sección 7). El análisis de cadenas de bloques, junto con las técnicas de investigación tradicionales puede permitir a los investigadores obtener la información necesaria para identificar a los delincuentes de *ransomware* en línea y a sus afiliados, así como rastrear el movimiento de los ingresos ilícitos.

71. El rastreo de ingresos mediante el análisis de cadena de bloques suele requerir la identificación de una dirección inicial de monedero, por lo que la detección y recopilación de información sobre el pago del rescate constituyen un primer paso fundamental. Una vez que se detecta una dirección inicial de monedero, los investigadores pueden identificar los pagos realizados y recibidos por esa dirección de monedero. Sin embargo, la información disponible puede depender del servicio que se utilice. Aunque la cadena de bloques pública contiene información útil para las investigaciones financieras, algunas transacciones de activos virtuales se producen fuera

de dicha cadena. Algunos análisis de cadenas de bloques se basan igualmente en algoritmos de agrupamiento y otras técnicas para conformar direcciones de monederos o transacciones que puedan estar asociadas a actividades delictivas, como el *ransomware*.

72. La información proveniente del análisis de cadena de bloques puede fortalecer aún más las técnicas de investigación tradicionales. Por ejemplo, el análisis de cadena de bloques podría ayudar a identificar un PSAV que aloje una dirección de monedero que haya recibido un pago enviado a o por delincuentes de *ransomware*, lo que podría llevar a las APJs a utilizar métodos obligatorios para solicitar información sobre la dirección del monedero al respectivo PSAV.

Recuadro 18. Investigaciones sobre monederos de *ransomware* conocidos revelan más víctimas desconocidas

Se habían estado realizando análisis de amenazas de cadenas de bloques en línea sobre una dirección de bitcoin de la que se sabía que había recibido aproximadamente 20 bitcoines entre el 12 de mayo de 2017 y el 27 de mayo de 2021. Se descubrió que dicha dirección podría estar directamente relacionada con un *ransomware* que infectó a varias entidades empresariales y gubernamentales de Sudáfrica. Los análisis revelaron que otra dirección local de bitcoin que pertenecía a un PSAV de Sudáfrica, proporcionó 0.06 bitcoines a la dirección antes mencionada sometida a investigación en febrero de 2018.

Tras obtener información sobre los suscriptores del PSAV, se identificó a una víctima que reconoció haber sufrido pérdidas económicas. Esta prefirió no denunciar el incidente a las autoridades locales de investigación por temor a la vergüenza pública de proteger de manera deficiente los datos de sus clientes. El asunto fue remitido por la UIF de Sudáfrica a las autoridades locales de investigación. Dado que la víctima identificada no quiso presentar cargos penales, las APJs locales retiraron y cerraron el caso.

Fuente: Sudáfrica.

73. Los métodos de LD que refuerzan el anonimato y son utilizados por los ciberdelincuentes dedicados al *ransomware* (analizados anteriormente en la sección 3) también plantean retos a las APJs para rastrear y asignar transacciones utilizando el análisis de cadena de bloques, aunque algunas empresas de análisis de cadena de bloques han desarrollado tecnología para mitigar algunas de estas medidas. Los modelos de afiliación o los proveedores de RaaS, así como la complicidad de mulas de dinero, también aumentan la complejidad de las investigaciones financieras relacionadas con el *ransomware*. Dado que los pagos no siempre pueden rastrearse hasta la víctima, resulta difícil identificar las direcciones utilizadas para el pago inicial de los activos virtuales, que suelen servir como pistas para el análisis de cadena de bloques.

74. Más allá de utilizar el análisis de cadena de bloques para rastrear el pago del ataque de *ransomware* y su posterior lavado, los investigadores igualmente deberían rastrear las transacciones anteriores asociadas con el grupo de *ransomware*. Este paso adicional permitiría a las APJs identificar posibles tendencias y tipologías, y/o delincuentes adicionales.

75. Como buena práctica, las APJs de ciertas jurisdicciones han desarrollado bases de datos con información clave sobre mulas de dinero o direcciones de monederos implicadas en casos de *ransomware*. Dichas bases de datos suelen incluir información sobre incidentes, que permite identificar mulas de dinero, el monto de los daños y los

delincuentes de *ransomware* (por ejemplo, número de cuenta, direcciones de monedero, nombres de usuario) Estas bases de datos ayudan a identificar y rastrear los pagos de *ransomware* y el LD relacionado a este, proporcionando un repositorio para comparar las pistas de investigaciones anteriores (incluyendo información sobre los pagos) con incidentes actuales y futuros. Esto permite a las APJs entender el funcionamiento de la red de LD más amplia establecida, la cual puede abarcar varias entidades y sectores regulados.

Recuperación de activos

76. Además de mejorar las técnicas de detección e investigación financiera, las APJs también necesitan contar con los poderes legales y la capacidad para asegurar y confiscar activos virtuales. Las transacciones de activos virtuales son casi instantáneas, por lo que tan pronto como las autoridades competentes tienen conocimiento de un ataque de *ransomware* y del consecuente pago de rescate, deben ser capaces de rastrear rápidamente este último y estar facultadas para congelar rápidamente las cuentas relacionadas, idealmente en cuestión de horas, para evitar su disipación. En línea con la Recomendación 4 del GAFI, dichas facultades deberían ya estar vigentes en muchas jurisdicciones y pueden variar en forma.

77. Varias jurisdicciones también destacaron la utilidad de utilizar herramientas alternativas para interceptar los ingresos ilícitos, como las facultades de aplazamiento de las UIF, para manejar los presuntos activos de origen criminal identificados en los ROS. Para lograr una actualización a la par del ritmo de dinamismo de los activos virtuales, es igualmente necesario actualizar la legislación, los reglamentos, así como las políticas y procedimientos existentes de incautación de activos.

Recuadro 19. El oleoducto *Colonial Pipeline*

En junio de 2021, el Departamento de Justicia de Estados Unidos anunció que había asegurado 63.7 bitcoines valorados en aproximadamente 2.3 millones de dólares. Estos fondos representaban supuestamente el importe del pago de rescate del 8 de mayo de 2021 a individuos de un grupo conocido como *DarkSide,* cuyo objetivo había sido el oleoducto *Colonial Pipeline*, dejando infraestructuras críticas fuera de funcionamiento. La orden de incautación fue autorizada por un juez del estado de California ese mismo día.

El 7 de mayo de 2021, o alrededor de esa fecha, *Colonial Pipeline* fue víctima de un ataque de *ransomware* muy mediático que hizo que la empresa dejara de operar parte de su infraestructura. *Colonial Pipeline* informó al FBI sobre una organización llamada *DarkSide,* la cual accedió a su red informática y por la que recibió y realizó un pago de rescate de aproximadamente 75 bitcoines. Como se alegó en la declaración jurada de apoyo, al revisar el registro público de Bitcoin, las APJs pudieron rastrear múltiples transferencias de bitcoines e identificar que aproximadamente 63.7 de estos, que representaban el importe del pago del rescate de la víctima, habían sido transferidos a una dirección específica. Este bitcoin representa ingresos rastreables por intrusión informática y propiedad involucrada en LD y puede ser asegurado de acuerdo con los estatutos de confiscación penal y civil.

Fuente: Estados Unidos.

Acciones propuestas

- Las autoridades competentes deben utilizar y adaptar, según sea necesario, las técnicas tradicionales de procuración de justicia, así como técnicas específicas de activos virtuales, para llevar a cabo investigaciones de LD relacionadas con *ransomware*.
- Las jurisdicciones deben garantizar que las APJs cuenten con y mantengan las habilidades y facultades necesarias para asegurar y confiscar activos de manera rápida y efectiva, en particular activos virtuales.

Habilidades y experiencia

78. Como se explica en la sección 6.2, si bien las técnicas tradicionales de cumplimiento de la ley siguen siendo fundamentales para las investigaciones de LD relacionadas con *ransomware*, también se requieren conocimientos técnicos especializados para garantizar el éxito de las investigaciones y los enjuiciamientos por LD, así como para recuperar los bienes relacionados con activos virtuales. Esto incluye el conocimiento tecnológico y legal del ecosistema de los activos virtuales.

79. Adicionalmente, los equipos de investigación que trabajen en casos de LD o recuperación de activos relacionados con *ransomware* deben incluir personal con habilidades técnicas en ciberseguridad, informática forense, inteligencia digital y plataformas de código abierto. Lo anterior incluye un enfoque de reconocimiento en línea para recopilar información financiera relativa a transacciones de activos virtuales dentro del dominio público, incluyendo información que puede identificarse mediante el análisis de cadena de bloques, el escaneo de sitios web, redes sociales, foros en línea, de la *dark web* y los mercados negros, así como las denuncias de abuso en línea.

80. Particularmente en el caso de activos virtuales, las autoridades competentes pueden requerir de nuevas habilidades y experiencia para interpretar y acceder a la información. Específicamente, deben estar familiarizadas con herramientas analíticas y de supervisión de cadenas de bloques, incluyendo el software libre para acceder a la cadena de bloques pública, y el análisis para rastrear fondos. Existen distintas herramientas adicionales que pueden proporcionarles técnicas diversas y complementarias (tales como el análisis de distintos tipos de activos virtuales, la capacidad de analizar saltos de cadena, la inteligencia de código abierto, etc.).

81. Se requiere formación especializada y conocimientos técnicos para desarrollar dichas herramientas y utilizarlas durante las investigaciones, y algunas jurisdicciones han identificado formas de integrar a especialistas en investigaciones relevantes (ver sección 8.2). Acceder a los recursos necesarios pudiera ser costoso y algunas jurisdicciones pueden carecer de ellos para promover el desarrollo de dichas competencias, lo cual puede obstaculizar la capacidad de las autoridades para perseguir el LD relacionado con el *ransomware*.

82. Si no existe experiencia propia o esta es insuficiente, las jurisdicciones pueden recurrir al uso de herramientas creadas por empresas del sector privado. Las herramientas de terceros pueden ayudar a las autoridades a identificar, rastrear y relacionar transacciones de activos virtuales en todas las principales cadenas de transacciones de activos virtuales y en la mayoría de las menores. Actualmente, dichas herramientas soportan cientos de *tokens* y utilizan métodos como algoritmos de agrupamiento, recopilación de información (*web scraping*), y la supervisión de bases

de datos de estafas que permiten a los investigadores vincular y atribuir una amplia gama de transacciones a personas y entidades del mundo real. Las herramientas generan gráficos de transacciones y posibilitan el análisis de redes, permitiendo a las agencias comprender y posteriormente presentar las complejas asociaciones a jurados y tribunales en los subsecuentes juicios y acciones de recuperación de activos. Estas herramientas también pueden ayudar a las autoridades a identificar los PSAV que pudieran haber sido utilizados para lavar o intercambiar ganancias ilícitas por moneda fiduciaria y que pueden constituir información relevante para apoyar la investigación.

83. En términos de recuperación de activos, el aseguramiento y la gestión de activos virtuales requieren conocimientos técnicos y legales adicionales. Las autoridades deben estar preparadas para tomar las medidas apropiadas y aplicar procedimientos que garanticen un aseguramiento y almacenamiento adecuados. Una buena práctica es establecer mecanismos especializados para asegurar, confiscar y disponer de activos virtuales. Lo anterior incluye la planeación adecuada del aseguramiento, la gestión de las frases semilla[37] y el almacenamiento en frío de los activos virtuales asegurados (es decir, almacenarlos en una billetera no alojada sin conexión), así como cuestiones relacionadas con la cadena de custodia.

Acciones propuestas

- Las autoridades competentes deben tener conocimiento especializado y la experiencia necesaria para que las investigaciones financieras relacionadas con *ransomware* sean exitosas. Ello incluye el desarrollo, acceso y la capacitación en herramientas de análisis y supervisión de cadenas de bloques.
- Las jurisdicciones deben garantizar la existencia de mecanismos especializados para gestionar adecuadamente los activos virtuales asegurados.

Políticas nacionales y coordinación

Evaluación y estrategia nacional

84. La Recomendación 1 del GAFI insta a las jurisdicciones identificar y evaluar sus riesgos de LD así como aplicar un enfoque basado en riesgos para lograr su mitigación. Dicho enfoque debe igualmente servir como base para que las jurisdicciones asignen eficientemente los recursos en su régimen ALD/CFT.

85. El *ransomware* a menudo se aborda desde la perspectiva de evaluación de amenazas a la ciberseguridad. Por ejemplo, a nivel nacional, algunas jurisdicciones han promulgado estrategias nacionales sobre ciberseguridad o ciberdelincuencia que apoyan la coordinación nacional y establecen el compromiso político para perseguir activamente el *ransomware* y los flujos financieros ilícitos asociados a este. Las estrategias nacionales suelen implicar a varios organismos gubernamentales[38] y pueden incluir a autoridades competentes en materia de ALD/CFT, como los ministerios de Justicia, Hacienda y del Interior, así como al sector privado. Sin embargo, es importante señalar que el propósito de muchas de estas estrategias no

[37] Conjunto de palabras generadas aleatoriamente por una aplicación de monedero y enumeradas en un orden específico que pueden utilizarse para recuperar o acceder a su(s) clave(s) privada(s) eludiendo la protección adicional (por ejemplo: la contraseña).

[38] Dichos organismos incluyen los relacionados con la procuración de justicia, defensa, seguridad y comunicación, dada la amenaza que el *ransomware* representa para la seguridad nacional.

necesariamente se centra en los riesgos del financiamiento ilícito, los cuales deben analizarse en detalle a través de una evaluación de riesgos.

Recuadro 20. Estrategia Nacional de Ciberseguridad de España

La Estrategia Nacional de Ciberseguridad de España (cuya última actualización fue en 2019) tiene como objetivo reforzar las técnicas para la lucha contra los ciberataques. Establece las prioridades, objetivos y medidas adecuadas para alcanzar y mantener un alto nivel de seguridad en las redes y los sistemas de información. Algunas de sus líneas de acción clave buscan fortalecer las competencias para combatir las ciberamenazas y reforzar las técnicas para investigar y procesar cualquier ciberdelito.

La Estrategia estableció la necesidad de reforzar la cooperación jurídica y policial, mediante la asignación de recursos suficientes a organismos competentes y el desarrollo de competencias profesionales. Lo anterior también está relacionado con la creación de un marco institucional para la ciberseguridad, en donde se definió la instauración del Consejo Nacional de Ciberseguridad. Dicho Consejo está dirigido por el primer ministro de España con el objetivo de coordinar la política de seguridad nacional en materia de ciberseguridad y promover la coordinación, colaboración y cooperación entre los organismos de la administración pública[1] y el sector privado[2], con un enfoque totalmente multidisciplinario.

Fuente: España.

Notas
1. Ministerios de Asuntos Exteriores, Justicia, Defensa, Asuntos Internos, Hacienda, Presidencia; el Centro Nacional de Inteligencia, el Departamento de Seguridad Nacional y otros.
2. Incluyendo aquellos provenientes de asociaciones profesionales, empresas y el mundo académico.

86. Las jurisdicciones deben asegurarse de que la amenaza de *ransomware* se incluya como parte de su evaluación nacional de riesgo de LD, conforme a la Recomendación 1 del GAFI. Esta evaluación proporciona la base sobre la que las jurisdicciones pueden construir medidas de mitigación - incluyendo la implementación de las acciones sugeridas presentadas en este informe. Una vez analizados y comprendidos los riesgos de LD asociados al *ransomware*, las jurisdicciones podrán asignar recursos en línea con un enfoque de administración de riesgos, incluyendo el desarrollo de habilidades y conocimientos técnicos de activos virtuales, así como de herramientas analíticas de cadenas de bloques para las respectivas autoridades competentes de ALD/CFT.

87. Las jurisdicciones en las que el *ransomware* y el LD asociado no representan actualmente una amenaza nacional deben igualmente considerar los riesgos de financiamiento ilícito planteados por el *ransomware*, en particular debido a la relación única entre este último y los activos virtuales. Las jurisdicciones deben considerar no sólo la amenaza de los ataques de *ransomware* para las víctimas nacionales, sino también la posibilidad de que los delincuentes de *ransomware* estén establecidos en sus jurisdicciones o que se estén utilizando los PSAV de sus jurisdicciones para lavar o cobrar las ganancias provenientes del *ransomware*. Por ejemplo, muchos PSAV pueden distribuir sus arquitecturas entre varias jurisdicciones, por ejemplo, registrándose en una jurisdicción, utilizando personal ubicado en otra jurisdicción, y alojando infraestructura técnica o claves privadas en jurisdicciones distintas. Lo anterior

significa que dichas jurisdicciones pueden seguir estando expuestas a movimientos financieros ilícitos relacionados con *ransomware*, especialmente a través de los PSAV.

Recuadro 21. Análisis de *ransomware* en las evaluaciones nacionales de riesgo de LD

En marzo de 2022, Estados Unidos publicó su tercera Evaluación Nacional de Riesgo de Lavado de Dinero (NMLRA, por sus siglas en inglés), en la que se destacan las amenazas financieras ilícitas más importantes, incluyendo el cibercrimen y las vulnerabilidades relacionadas con los activos virtuales. La NMLRA identificó que los incidentes de ciberdelincuencia aumentaron significativamente desde 2018, y que el *ransomware* representa una amenaza financiera ilícita particularmente significativa. Por ejemplo, la NMLRA descubrió que la gravedad y sofisticación de los ataques de *ransomware* aumentaron durante la pandemia de COVID-19. La NMLRA proporciona información sustancial sobre las tendencias de los ataques de *ransomware*, incluyendo el uso del RaaS y las tácticas de doble extorsión. La NMLRA también destaca numerosas tipologías de LD, como el uso de los PSAV extranjeros con controles de ALD/CFT débiles o inexistentes para depósitos relacionados con *ransomware*. Los hallazgos de la NMLRA se incluyeron como parte de los trabajos de la Estrategia Nacional para Combatir el Terrorismo y otras Finanzas Ilícitas de 2022, que proporciona recomendaciones para atender los riesgos relacionados con financiamiento ilícito, y del Plan de Acción para Combatir los Riesgos de Financiamiento Ilícito Proveniente de Activos Digitales.

Fuente: Estados Unidos.

Cooperación y coordinación nacional

88. La Recomendación 2 del GAFI establece que las jurisdicciones dispongan de mecanismos nacionales para que legisladores, la UIF, las APJs y otras autoridades competentes cooperen, se coordinen e intercambien información. El *ransomware* afecta a una amplia variedad de sectores y las investigaciones pueden involucrar a otros participantes además de las autoridades tradicionales de ALD/CFT, tales como las agencias de ciberseguridad y de protección de datos. El establecimiento de mecanismos de coordinación nacionales efectivos es vital para reunir información relevante y a diferentes expertos, incluyendo los del sector privado, para garantizar una respuesta holística/integral que mitigue la amenaza del *ransomware* y el LD asociado a este. Lo anterior a su vez permite el intercambio crítico de información entre las APJs que realizan investigaciones forenses determinantes e investigaciones paralelas de financiamiento.

89. Una buena práctica es la creación de equipos de procuración de justicia u organismos multidisciplinarios dedicados al cibercrimen (o incluso solo al *ransomware*). Estos órganos pueden coordinar investigaciones sobre *ransomware* y LD relacionado a este que requieran una amplia gama de conocimientos especializados (por ejemplo, expertos de la UIF o de APJs, fiscales, ingenieros técnicos, negociadores, etc.). Este enfoque suele incluir a funcionarios de las APJs con experiencia en rastreo de activos virtuales y puede ser una forma útil de centralizar los conocimientos técnicos especializados, particularmente ante la limitación de recursos o capacidades en las jurisdicciones.

Recuadro 22. Mecanismos de coordinación para centralizar la inteligencia y los conocimientos en técnicas de investigación

Para afrontar los riesgos cibernéticos en permanente evolución, el Gobierno de Estados Unidos creó en 2008 la *National Cyber Investigative Joint Task Force* (NCIJTF). La NCIJTF se encuentra conformada por más de 30 organismos asociados relacionados con las APJs, la comunidad de servicios de inteligencia y el Departamento de Defensa, y con representantes que trabajan de manera conjunta para cumplir la misión de la organización desde una perspectiva integral de gobierno.

Como centro cibernético multiinstitucional único, la NCIJTF tiene como principal responsabilidad coordinar, integrar y compartir información para apoyar las investigaciones sobre amenazas cibernéticas, proporcionar y respaldar el análisis de inteligencia para los responsables de la toma de decisiones, y aportar valor a otros esfuerzos en curso en la lucha contra la amenaza cibernética en Estados Unidos.

A finales de 2014, la NCIJTF creó el Equipo de Moneda Virtual (VCT, por sus siglas en inglés), el cual centró sus esfuerzos en rastrear transacciones de criptodivisas relacionadas con ciberdelitos. Este equipo proporciona información sobre el rastreo de criptomonedas a todos los miembros de la NCIJTF. Como parte de sus propios esfuerzos de investigación, miembros de la NCIJTF, tales como el FBI y el Servicio Secreto, crearon sus propios equipos para rastrear activos virtuales a medida que aumentaba su uso en diversos tipos de delitos.

A principios de 2022, el FBI creó la Unidad de Activos Virtuales (VAU, por sus siglas en inglés), un centro neurálgico para programas de moneda virtual del FBI en donde la inteligencia, la tecnología y el apoyo operativo servirán para atender igualmente otras divisiones. En la VAU, los expertos en activos virtuales y en recursos interdivisionales forman parte de un grupo de trabajo que integra plenamente la inteligencia y las operaciones en todo el FBI.

Fuente: Estados Unidos.

Cooperación con y guías para el sector privado

90. Como se indica en la sección 5.2, la colaboración con el sector privado es útil para mitigar algunos de los retos identificados en el presente informe. Por ejemplo, las entidades reguladas pueden tener dificultades para detectar e identificar operaciones sospechosas relacionadas con el *ransomware*. Algunas jurisdicciones han tenido éxito en mejorar la frecuencia y calidad de los informes de ROS relacionados con r*ansomware* al comprometerse y proporcionar orientación a sujetos obligados, incluyendo indicadores de alerta (ver *Countering Ransomware Financing: Potential Risk Indicators*, FATF, 2023, disponible en inglés) y guías de detección.

Recuadro 23. Guías sobre delitos financieros en Australia

La Alianza Fintel de Australia[1] publica una serie de recursos, incluyendo guías sobre delitos financieros, para ayudar a las empresas a comprender, identificar y notificar actividades financieras sospechosas para detectar y prevenir actos delictivos.

Las guías sobre delitos financieros ofrecen información detallada sobre los aspectos financieros de distintos tipos de delitos. Incluyen estudios de caso e indicadores para ayudar al sector de servicios financieros a identificar y detectar transacciones sospechosas.

Para colaborar en la lucha contra el *ransomware*, la Unidad de Inteligencia Financiera de Australia, mejor conocida como AUSTRAC, publicó en abril de 2022 una serie de guías de delincuencia financiera sobre el uso indebido de monedas digitales, así como la identificación y detención del *ransomware*. Ambas guías proporcionan información práctica e indicadores clave de riesgo para ayudar a detectar y responder cuando alguien pueda ser blanco de un pago de *ransomware* o esté intentando beneficiarse de ello. Ambas guías sobre delitos financieros están disponibles en el sitio web de AUSTRAC:

- *Detecting and stopping ransomware payments | AUSTRAC*
- *Preventing the criminal abuse of digital currencies | AUSTRAC*

Fuente: Australia.

1. La Alianza Fintel es una asociación público-privada de Australia que reúne a expertos de diversas organizaciones dedicadas a la lucha contra el LD, el financiamiento del terrorismo y otros delitos graves. Entre los socios de la Alianza figuran grandes bancos, proveedores de servicios de remesas y operadores de apuestas, así como APJs y agencias de seguridad australianas y extranjeras.

91. La forma y grado de colaboración con el sector privado para combatir el *ransomware* varía según las jurisdicciones. Las asociaciones público-privadas (APP) son un modelo útil y comúnmente entendido, aunque en muchas jurisdicciones siguen centrándose en las partes interesadas tradicionales (en particular, los bancos y otras instituciones financieras, aunque cada vez existe una mayor participación de las APNFD). La composición específica varía dependiendo de los fines y objetivos de la APP, pero puede incluir a partes interesadas no tradicionales. En el contexto de la prevención y detección efectiva del *ransomware*, las APP deben utilizarse para reunir a las APJs, el EREI local, la UIF y los PSAV, además de las empresas de ciberseguridad, los proveedores de telecomunicaciones y las empresas de análisis de cadenas de bloques (por ejemplo, como un subgrupo o brazo operativo de una APP existente).

92. Entre los objetivos comunes de las APP figuran sensibilizar a los participantes sobre el *ransomware* y el LD asociado a este, intercambiar información sobre tendencias actuales, y explorar amenazas nuevas y existentes. Estos mecanismos pueden consolidar relaciones más sólidas con el sector privado y fomentar las denuncias.

93. Las jurisdicciones también han aprovechado las APP para alcanzar diversos objetivos en materia de procuración de justicia. Las APP ofrecen una plataforma útil para compartir información táctica a fin de generar inteligencia, permitir el intercambio de información para mejorar la detección de redes de mulas de dinero y LD en diversos sectores regulados y avanzar en las investigaciones.

94. Dado que los PSAV disponen de información clave para una procuración de justicia exitosa (incluyendo la titularidad de monederos y retiros en moneda fiduciaria), el desarrollo de relaciones de cooperación con este sector puede permitir a las autoridades acceder rápidamente a información para rastrear activos virtuales, y proceder a una incautación y confiscación efectiva.

Recuadro 24. Proyecto GATEWAY y Operación Ciclón de INTERPOL

El Proyecto GATEWAY es un marco de intercambio de datos con entidades privadas que inició en 2016 para intercambiar información relacionada con el cibercrimen. El proyecto promueve la colaboración entre las APJs y la industria privada para generar datos sobre amenazas a partir de diversas fuentes y permitir a las autoridades policiales prevenir ciberataques. Las entidades que forman parte del Proyecto son actores relevantes en el ecosistema del cibercrimen. Entre ellos se encuentran empresas de ciberseguridad, empresas de inteligencia de amenazas, PSAV y bancos.

El marco permite el suministro y recepción de información sobre ciberdelincuencia entre INTERPOL y el sector privado, y permite a este último proporcionar asistencia a INTERPOL para analizar el cibercrimen. Los socios del sector privado apoyan tanto con sus conocimientos técnicos para ayudar a determinar los tipos de infección por *ransomware*, como con el análisis de cualquier posible pista para relacionar transacciones.

La Operación Ciclón[1] da seguimiento a las investigaciones policiales globales sobre ataques contra empresas coreanas e instituciones académicas estadounidenses perpetrados por el grupo de amenaza de *ransomware* Cl0p. La operación global de junio de 2021 resultó en la detención de seis miembros de dicho grupo, y fue coordinada por INTERPOL con la participación de las APJs de Corea, Ucrania y Estados Unidos. Se cree que los sospechosos han facilitado la transferencia y el cobro de activos con un valor de más de 500 millones de dólares estadounidenses en nombre del grupo que se dedicaba a la extorsión. INTERPOL desplegó la Operación Ciclón con la ayuda de información facilitada por sus socios privados a través del Proyecto Gateway de INTERPOL.

Fuente: INTERPOL.

1. Para mayor información, consultar: www.interpol.int/en/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring

Acciones propuestas

- Las jurisdicciones deben asegurarse de identificar y evaluar los riesgos de LD planteados por *ransomware* en sus evaluaciones de riesgos nacionales. Dada la naturaleza descentralizada de los activos virtuales y de los grupos delictivos de *ransomware*, lo anterior incluye jurisdicciones con sectores de activos virtuales en los que el *ransomware* actualmente no constituye una amenaza nacional. Estos hallazgos pueden ayudar a fortalecer las estrategias nacionales de ciberseguridad a través de una visión holística/integral nacional de riesgos de *ransomware*.
- Las jurisdicciones deben desarrollar mecanismos de coordinación entre las autoridades competentes pertinentes, desde las APJs, ALD/CFT y autoridades en contra del cibercrimen, hasta socios no tradicionales como las agencias de ciberseguridad o de protección de datos. Ello fomenta el intercambio de información e inteligencia y proporciona una plataforma útil para intercambiar diversos conocimientos técnicos.
- Las jurisdicciones deben identificar y establecer mecanismos para fortalecer la cooperación público-privada. Las jurisdicciones deben considerar la inclusión de los PSAV y otros socios no tradicionales en dichos mecanismos de cooperación.

Cooperación internacional

95. Los ataques de *ransomware* así como los flujos financieros relacionados suelen ser transnacionales y multinacionales. Los delincuentes de *ransomware* suelen estar ubicados en una jurisdicción distinta de las múltiples jurisdicciones a través de las cuales se lavan y cobran los fondos (en particular, los activos virtuales). La complejidad y los retos de los esquemas de LD relacionados con *ransomware* requieren una cooperación transfronteriza continua entre las APJs que proporcionen información, herramientas y conocimientos relevantes. Es imprescindible crear y aprovechar los mecanismos existentes de cooperación internacional para lograr investigaciones financieras, así como una recuperación de activos exitosas, especialmente en los casos de *ransomware*.

Recuadro 25. Investigación internacional conjunta contra la variante Lockergoga

En enero de 2019 se produjo un ataque de *ransomware* contra una importante empresa francesa. El malware Lockergoga fue identificado como una variante de r*ansomware* utilizada para cifrar varios archivos y servidores internos de la empresa. Aunque se solicitó un rescate de 410 bitcoines, la empresa no pagó el rescate. Sin embargo, también se descubrió que dicha variante había sido empleada por hackers en otros numerosos ataques.

Se formó un equipo conjunto de investigación bajo el mando de Eurojust/Europol en coordinación con varias jurisdicciones europeas. Ello dio lugar a un intercambio eficaz de información, incluyendo la cooperación jurídica a través de las Órdenes Europeas de Investigación (*EIO*, por sus

siglas en inglés) y el Tratado de Acuerdo Jurídico Mutuo (*MLAT*, por sus siglas en inglés), lo que contribuyó a agilizar las investigaciones. Europol/Eurojust también proporcionó apoyo técnico con gran capacidad de hardware y financiamiento. Posteriormente se identificó una infraestructura de mando y control criminal, con flujos de mensajería descifrados de los hackers, y finalmente se descubrió que el grupo estaba ubicado en una jurisdicción de Oriente. Ello permitió realizar varias detenciones en dicha jurisdicción.

Las investigaciones continúan. Mediante el análisis de cadenas de bloques, los investigadores desentrañaron las diversas técnicas de cadenas de transacciones utilizadas. Lo anterior derivó en la detención de uno de los principales lavadores de dinero en Suiza. También se detuvieron a otras mulas de dinero en distintas jurisdicciones. Las investigaciones revelaron que los rescates pagados no estaban destinados para beneficiar exclusivamente al hacker. Por ejemplo, pagos ilícitos fueron realizados a varios socios criminales y utilizados para la infraestructura (ingenieros y desarrolladores de software, ordenadores *host* blindados para servidores seguros, servicios de VPN blindados para ocultar la comunicación o conexión con los servidores de mando y control, servicios de LD para organizar los movimientos de cadenas de transacciones, etc.), y para encontrar mulas de dinero e instalaciones de cobro.

Fuente: Francia.

96. La información solicitada en las peticiones internacionales suele referirse tanto a las pruebas forenses necesarias para las investigaciones determinantes como a datos financieros necesarios para las investigaciones de LD. Esto incluye direcciones IP situadas en el extranjero, nombres y alias utilizados, información sobre suscriptores, así como información sobre beneficiarios finales, detalles de transacciones e información de contrapartes relacionada con monederos alojados en PSAV extranjeros.

Retos específicos planteados por el uso de activos virtuales

97. El uso de activos virtuales en el LD relacionado con *ransomware* puede plantear nuevas dificultades para la cooperación transfronteriza. Las diferencias en el tratamiento sustantivo o la regulación de los activos virtuales en los distintos sistemas legales -y la escasa o nula participación o supervisión gubernamental del sector en algunas jurisdicciones- pueden complicar la capacidad o la disposición de las autoridades de participar en la cooperación internacional.

98. Por ejemplo, las jurisdicciones que no registran o supervisan a los PSAV pueden tener dificultades para identificar a las empresas a las cuales solicitan información. Incluso si se localiza a la entidad apropiada, las autoridades pueden tener acceso únicamente a técnicas de investigación coercitivas para ejecutar una solicitud de cooperación internacional. Esto puede limitar la información que puede obtenerse mediante procesos de cooperación informal.

99. Este reto se ve agravado por el hecho de que muchas jurisdicciones en las que se ubican los delincuentes de *ransomware* y sus mulas de dinero, o en las que operan PSAV que son utilizados para lavar y cobrar sus ganancias, son tolerantes con esta actividad y pueden no responder a solicitudes por parte de las APJs extranjeras. Cuando los PSAV se encuentran en jurisdicciones sin obligaciones en materia de ALD/CFT, es posible que simplemente no cuenten con los registros pertinentes para disposición de las APJs. En última instancia, esto frustra las investigaciones

financieras en curso y los intentos de recuperación de activos. Estos retos refuerzan cada vez más la importancia de acelerar la implementación global de la Recomendación 15 del GAFI (incluyendo la regla de viaje).

Recuadro 26. Retos de investigación planteados por un PSAV no cooperativo en el extranjero

La empresa X fue víctima de un ataque de *ransomware*, que presumiblemente era del tipo Caley. Después de negociar, la víctima pagó 0.25 bitcoines al delincuente de *ransomware* y recibió un correo electrónico con la clave de descifrado, lo que permitió que las operaciones de la víctima volvieran a la normalidad tras el proceso de descifrado.

Las autoridades tuvieron conocimiento del caso de forma tardía a través de una denuncia policial presentada por la víctima varios días después de pagar el rescate, lo que provocó que el rastro del pago fuera volviéndose menos perceptible. Según el análisis de cadenas de bloques, el rastro del pago del rescate terminó en un PSAV con sede en el extranjero, y se observó que un saldo de 0.0081 bitcoines fue a parar a un monedero alojado por el PSAV extranjero, que desde entonces se ha mantenido renuente a proporcionar información a pesar de las múltiples peticiones realizadas. Las investigaciones se complicaron aún más ya que el perpetrador utilizó un mezclador para ocultar las transacciones. Dadas las circunstancias de este caso, el agresor sigue siendo desconocido y no se ha podido recuperar ningún activo ni proceder a ninguna detención.

Fuente: Singapur.

100. Las arquitecturas distribuidas de algunos PSAV (con operaciones en múltiples jurisdicciones) también pueden representar una importante carga de investigación para las APJs al momento de identificar la entidad adecuada a la cual dirigirse para solicitar información, o la jurisdicción adecuada a la cual enviar una solicitud de colaboración. Por ejemplo, una jurisdicción citó dificultades para identificar la jurisdicción pertinente a la cual solicitar colaboración basándose en un Código Internacional de Cuenta Bancaria (IBAN, por sus siglas en inglés) que presumiblemente pertenece a una cuenta bancaria gestionada por un PSAV en una institución financiera extranjera. Otra jurisdicción señaló que algunos PSAV parecen no tener presencia física, lo que dificulta identificar las jurisdicciones adecuadas con las cuales establecer esquemas de cooperación.

La necesidad de una cooperación rápida

101. Dado que los delincuentes de *ransomware* pueden estar distribuidos alrededor del mundo y los activos virtuales pueden transferirse casi instantáneamente, las APJs necesitan actuar con rapidez para rastrear y prevenir la dispersión transfronteriza de las ganancias provenientes del *ransomware*. Para ello, se requieren mecanismos formales de cooperación internacional (como la asistencia legal mutua) para obtener pruebas y asegurar incautaciones en el contexto de procesos penales. Sin embargo, los mecanismos formales de cooperación no siempre propician la rapidez, lo que puede retrasar, detener o incluso frustrar considerablemente las investigaciones. La complejidad de las investigaciones relacionadas con *ransomware*, en cuanto al número de jurisdicciones y empresas implicadas, acentúa estos retos, ya que las operaciones de cooperación internacional requieren más tiempo y recursos para casos de *ransomware* que de otras actividades delictivas.

102. Aprovechar la cooperación informal puede ser útil para superar estos retos y ayudar a simplificar y agilizar las solicitudes de asistencia legal mutua. Para facilitar una cooperación oportuna, algunas jurisdicciones señalaron la importancia de los contactos existentes y establecieron canales informales para contactar y relacionarse con contrapartes extranjeras. Esto ayuda a facilitar un intercambio rápido de información necesaria para avanzar en los procedimientos penales, respetando al mismo tiempo los procesos necesarios para proteger dicha información. Este intercambio informal de información puede producirse entre las UIF a través de la red segura de Egmont, mientras que la cooperación entre policías puede darse a través del sistema I-24/7 de INTERPOL, así como de otras redes informales, como la Red Interinstitucional de Recuperación de Activos de Camden (CARIN, por sus siglas en inglés) y las redes interinstitucionales regionales de recuperación de activos (ARIN, por sus siglas en inglés). Las autoridades deben contar con procesos y puntos de contacto para los canales de cooperación internacional y regional disponibles para localizar rápidamente los fondos y lograr una recuperación efectiva de activos.

103. Algunas jurisdicciones han tenido éxito cooperando a través de relaciones bilaterales. El uso de oficiales de enlace dedicados a ciberdelitos a nivel internacional puede facilitar significativamente el intercambio de información e inteligencia entre el servidor (*host*) del enlace y la jurisdicción local, así como permitir a las autoridades recopilar y proporcionar evidencia del extranjero en investigaciones relacionadas con *ransomware*. Para promover la cooperación bilateral, las autoridades deben considerar hacer públicos los procesos y puntos de contacto para la cooperación, particularmente para apoyar el rastreo rápido de fondos y la recuperación de activos.

Recuadro 27. Proyecto CODA

En noviembre de 2021 se detuvo a un ciberdelincuente canadiense relacionado con campañas de *ransomware* e intrusiones cibernéticas en oficinas gubernamentales e instalaciones médicas de Alaska, Estados Unidos, acusado de múltiples delitos cibernéticos. Antes de ponerse en contacto con socios internacionales, el FBI estaba investigando varias intrusiones cibernéticas delictivas relacionadas. Una vez identificado y localizado el sujeto, el FBI se puso en contacto con su contacto bilateral en la Policía Provincial de Ontario (OPP, por sus siglas en inglés).

Se iniciaron investigaciones paralelas en ambas jurisdicciones, con apoyo del Centro Nacional Canadiense de Coordinación del Cibercrimen (NC3), Europol y las APJs danesas, proporcionando asistencia directamente a la OPP y al FBI. El NC3 ofreció apoyo operativo, análisis de datos y conductual, resúmenes e informes de inteligencia, y servicios de localización de criptomonedas a lo largo de 23 meses como parte de la investigación internacional. Dichos esfuerzos ayudaron a identificar al sujeto de interés, lo que condujo a su posterior arresto. El uso de técnicas analíticas avanzadas y herramientas especializadas como el rastreo de criptomonedas es clave en este tipo de investigaciones de ciberdelincuencia.

Fuente: Canadá y Estados Unidos.

Importancia de la coordinación multilateral

104. En los estudios de caso en los que se han aplicado medidas coercitivas de manera exitosa suelen participar autoridades competentes de varias jurisdicciones. Esto refleja la naturaleza internacional y descentralizada de los ataques de *ransomware* y el LD asociado a este. Un elemento para el éxito de dichas medidas es la necesidad de establecer una coordinación internacional entre las jurisdicciones afectadas para desarraigar y desarticular simultáneamente los sindicatos cibernéticos y sus afiliados. Esto también reduce el riesgo de desplazamiento, en donde estas organizaciones criminales pueden reubicar fácilmente sus operaciones digitales a otro refugio seguro.

105. Existen varios mecanismos internacionales de coordinación de las APJs que pueden utilizarse con este fin, como Europol/Eurojust o INTERPOL. Estas organizaciones albergan bases de datos y proporcionan logística y experiencia para coordinar a las partes interesadas de varias jurisdicciones. Dichos mecanismos multilaterales pueden ser útiles, especialmente para acelerar el intercambio de información crítica para las investigaciones financieras y la recuperación de activos.

Recuadro 28. Operación GoldDust[1]

En noviembre de 2021, las autoridades rumanas detuvieron a dos individuos sospechosos de ataques cibernéticos con *ransomware* tipo Sodinokibi/REvil. Presuntamente son responsables de 5,000 infecciones, que en total representaron el pago de medio millón de euros en rescates. Desde febrero de 2021, las APJs también han detenido a otros tres afiliados de Sodinokibi/REvil y a dos sospechosos relacionados con el *ransomware* GandCrab. Estos son algunos de los resultados de la operación GoldDust, en la que han participado 17 jurisdicciones[2], Europol, Eurojust e INTERPOL. Todas las detenciones se produjeron posterior a los esfuerzos conjuntos de las APJs internacionales de identificar, intervenir las comunicaciones telefónicas y asegurar parte de la infraestructura utilizada por la familia del *ransomware* Sodinokibi/REvil, considerada como sucesora de GandCrab.

La operación GoldDust se desarrolló a partir de pistas relacionadas con investigaciones anteriores dedicadas a GandCrab, una investigación dirigida por Rumania con el apoyo de Europol y APJs de varias jurisdicciones, entre ellas el Reino Unido y Estados Unidos.

Europol facilitó el intercambio de información, apoyó la coordinación de la operación GoldDust y proporcionó apoyo analítico operativo, así como el análisis de criptomonedas, programas maliciosos y forense. Europol también desplegó expertos en cada lugar y activó un puesto de mando virtual para coordinar las actividades de campo. La cooperación internacional permitió a Europol optimizar los esfuerzos de mitigación de las víctimas con otras jurisdicciones de la UE. Estas actividades evitaron que otras empresas privadas fueran víctimas del *ransomware* Sodinokibi/REvil.

El Grupo Operativo Conjunto de Acción contra el Cibercrimen (J-CAT, por sus siglas en inglés) de Europol apoyó la operación. Este equipo operativo fijo está compuesto por funcionarios de enlace cibernético de diferentes jurisdicciones que trabajan desde la misma oficina en investigaciones de ciberdelincuencia de alto nivel.

Fuente: Europol.

Notas

1. Para mayor información, consultar: www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged
2. Jurisdicciones participantes: Alemania, Australia, Bélgica, Canadá, Corea del Sur, Estados Unidos, Filipinas, Francia, Kuwait, Luxemburgo, Noruega, Países Bajos, Polonia, Reino Unido, Rumanía, Suecia y Suiza.

Acciones propuestas

- Las jurisdicciones deben establecer y participar activamente en mecanismos bilaterales, regionales y multilaterales, a través del uso de oficinas de enlace y el establecimiento de puntos de contacto claros 24/7, para facilitar una cooperación internacional rápida y el intercambio de información.

Conclusiones

106. A pesar del reciente crecimiento de flujos financieros mundiales provenientes del *ransomware*, aún existe una falta de investigaciones sobre el LD asociado a este. El presente estudio ha demostrado que el *ransomware* es un problema multidisciplinario e internacional que requiere un enfoque coordinado para lograr una respuesta eficaz contra esta amenaza. Para ello, las jurisdicciones deben aprovechar la colaboración en tres niveles: público-público; público-privado; y con jurisdicciones extranjeras y organismos multilaterales.

107. El presente estudio ilustra aún más la importancia de implementar rápidamente los Estándares del GAFI para proporcionar un marco eficaz para combatir las ganancias ilícitas provenientes del *ransomware*, especialmente en relación con activos virtuales y los PSAV. El GAFI seguirá promoviendo la implementación de sus Estándares en este sector.

108. Finalmente, el papel de los activos virtuales en el lavado de ganancias provenientes del *ransomware*, así como la evolución de las técnicas empleadas por los grupos criminales de *ransomware*, plantean nuevos retos. Las autoridades competentes deben asegurarse de que sus leyes se encuentren debidamente actualizadas y de que igualmente consideren las habilidades y capacidades necesarias para hacer frente a un entorno delictivo digital y dinámico.

www.fatf-gafi.org

Marzo 2023

Countering Ransomware Financing: Potential Risk Indicators (disponible en inglés)

Estos indicadores de riesgo potencial ayudarán a las entidades de los sectores público y privado a identificar actividades sospechosas relacionadas con el *ransomware*. Dichos indicadores complementan el informe del GAFI *Combate Contra el Financiamiento del Ransomware*, que analiza los métodos que utilizan los delincuentes para llevar a cabo los ataques de *ransomware* y cómo se efectúan y blanquean los pagos.