FATF

REPORTE GAFI

Combate contra el financiamiento del *ransomware*

POTENCIALES INDICADORES DE RIESGO

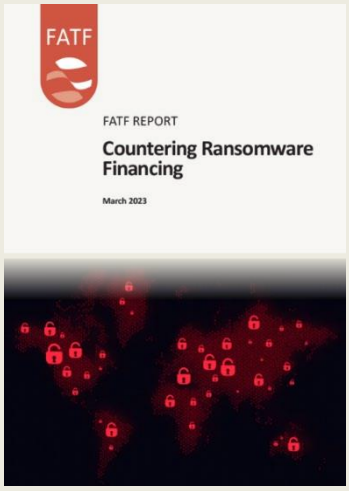
Marzo 2023

COMBATE CONTRA EL FINANCIAMIENTO DEL RANSOMWARE: POTENCIALES INDICADORES DE RIESGO

Los siguientes potenciales indicadores de riesgo se basan en la experiencia y los datos recibidos de jurisdicciones de toda la Red Global. El objetivo de estos indicadores es mejorar la detección de transacciones sospechosas relacionadas con el ransomware. La lista se diferencia además en varias perspectivas a lo largo de realizar un pago por ransomware.

Antes de utilizar los indicadores de riesgo, se recomienda a los lectores que lean las notas que figuran a continuación y el reporte 2023 del GAFI sobre el combate contra el financiamiento del ransomware.

Combate contra el Financiamiento del Ransomware



Este reporte analiza los métodos que utilizan los delincuentes para llevar a cabo sus ataques de ransomware y cómo lavan los pagos de los rescates.

El reporte destaca que las autoridades deben aprovechar los mecanismos de cooperación internacional existentes para hacer frente con éxito al lavado de los pagos por ransomware. También necesitan desarrollar las capacidades y herramientas necesarias para recopilar rápidamente información clave, rastrear las transacciones virtuales casi instantáneas y recuperar los activos virtuales antes de que se disipen.

https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/countering-

La existencia de un único indicador en relación con un cliente o una transacción puede no justificar por sí sola la sospecha de un delito de ransomware, así como tampoco un indicador por sí solo proporcionará necesariamente una indicación clara de tal actividad. Sin embargo, podría dar lugar a una mayor supervisión y examen, según proceda.

La lista de indicadores complementa los que figuran en los Indicadores de Alerta de Activos Virtuales del GAFI[1], y es pertinente tanto para el sector público como para el privado. En este último, los indicadores pueden ser pertinentes para los PSAV, los bancos y otras instituciones financieras y de pago.

[1] Indicadores de Alerta de Lavado de Dinero de Activos Virtuales del GAFI (Septiembre 2020), disponible en: www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf

Bancos/Otras instituciones financieras y de pago que identifican el pago de víctimas de ransomware

- Transferencias bancarias salientes a empresas de consultoría de ciberseguridad o de respuesta a incidentes especializadas en la remediación de ransomware
- Transferencias bancarias entrantes inusuales de compañías de seguros especializadas en la remediación de ransomware
- Auto denuncia del cliente de un ataque de ransomware o pago
- Información de fuentes abiertas sobre ataques de ransomware a clientes
- Alto volumen de transacciones de una misma cuenta bancaria a múltiples cuentas en un PSAV
- La descripción del pago contiene palabras como “rescate” o nombres de grupos de ransomware
- Pagos realizados a PSAV en jurisdicciones de alto riesgo (ver recuadro)

PSAVs identifican el pago de las víctimas del ransomware

- Solicitud de compra de activos virtuales por parte de una empresa de respuesta a incidentes o una compañía de seguros en nombre de un tercero
- El cliente declara al PSAV que está comprando activos virtuales debido al pago de un ransomware
- Usuario sin historial en transacciones con activos virtuales que envía fondos fuera de las prácticas comerciales habituales
- Un cliente aumenta el límite de una cuenta y la envía a un tercero
- Un cliente parece ansioso o impaciente por el tiempo que tarda un pago
- Compras o transferencias de criptomonedas anónimas
- Pagos realizados a PSAVs en jurisdicciones de alto riesgo
- Un nuevo cliente compra activos virtuales y transmite todo el saldo de su cuenta a una única dirección

PSAVs que identifican el recibo de pago de ransomware/cuenta criminal de ransomware

- Tras una gran transferencia inicial de activos virtuales, el cliente tiene poca o nula actividad con criptoactivos
- El análisis de la cadena de bloque (blockchain) sobre las direcciones de los monederos virtuales revela vínculos con el ransomware
- Retiro inmediato luego de convertir los fondos a activos virtuales
- Envíos de activos virtuales a monederos virtuales relacionados con el ransomware
- Uso de un PSAV en una jurisdicción de alto riesgo
- Transferencia de activos virtuales al servicio de mezcla
- Uso de una red encriptada
- La información de verificación es una fotografía de datos en una pantalla de ordenador o tiene un nombre de archivo que contiene “imagen de Whatsapp” o similar
- La sintaxis del cliente no coincide con sus datos demográficos
- La información del cliente muestra que el cliente tiene una cuenta de correo electrónico conocida por su alta privacidad, como proton mail o Tutanota
- Detalles inconsistentes de identificación o un intento por crear una cuenta con una identidad falsa
- Múltiples cuentas vinculadas a los mismos datos de contacto; direcciones compartidas bajo diferentes nombres
- El cliente parece utilizar una VPN
- Transacciones que involucran criptomonedas anónimas

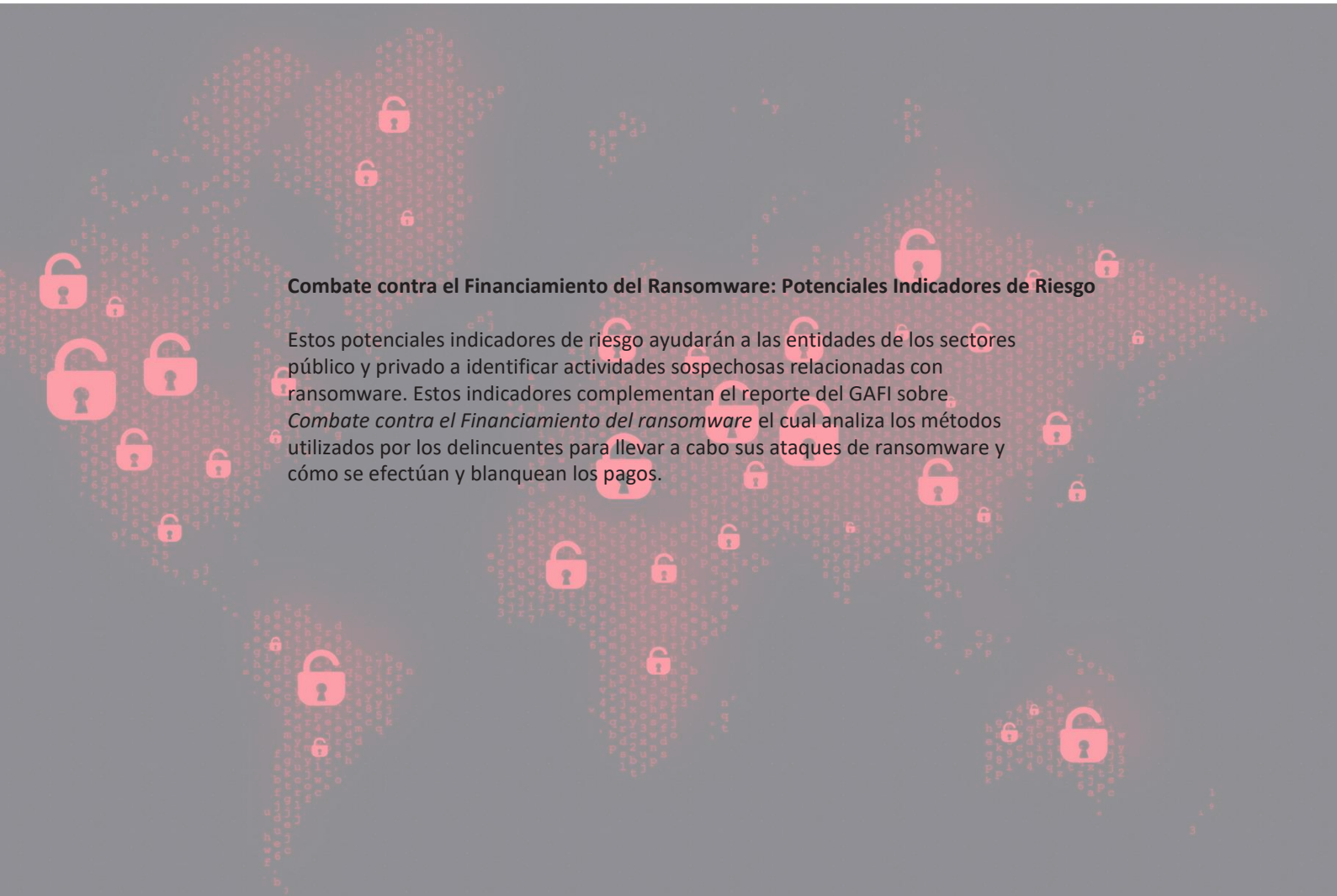
Recuadro: Jurisdicciones con mayor riesgo de lavado de dinero

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 áreas geográficas identificados por fuentes creíbles como proveedores de financiación o apoyo a actividades terroristas o que cuentan con organizaciones terroristas designadas que operan en ellos; (b) Países identificados por fuentes creíbles como poseedores de niveles significativos de delincuencia organizada, corrupción u otras actividades delictivas, incluidos los países de origen o tránsito de drogas ilegales, trata de personas, contrabando y juegos de apuesta ilegales; (c) Países que son objeto de sanciones, embargos o medidas similares emitidas por organizaciones internacionales como Naciones Unidas; y (d) Países identificados por fuentes creíbles como países con regímenes débiles en materia de gobernanza, aplicación de la ley y regulación, incluidos los países identificados por las declaraciones del GAFI como países con regímenes débiles en materia de ALD/CFT, especialmente para los PSAVs, y a los que los PSAVs y otros sujetos obligados deben prestar especial atención a sus relaciones y transacciones comerciales.

Fuente: GAFI (2021) Guía actualizada para un Enfoque Basado en Riesgo: Activos Virtuales y PSAVs, para. 154

www.fatf-gafi.org

Marzo 2023



Combate contra el Financiamiento del Ransomware: Potenciales Indicadores de Riesgo

Estos potenciales indicadores de riesgo ayudarán a las entidades de los sectores público y privado a identificar actividades sospechosas relacionadas con ransomware. Estos indicadores complementan el reporte del GAFI sobre *Combate contra el Financiamiento del ransomware* el cual analiza los métodos utilizados por los delincuentes para llevar a cabo sus ataques de ransomware y cómo se efectúan y blanquean los pagos.