UNODC
Oficina de las Naciones Unidas
contra la Droga y el Delito

DOCUMENTO DE POLÍTICA SOBRE LOS PROGRAMAS SECUESTRADORES

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO

Documento de política sobre los programas secuestradores

NACIONES UNIDAS
Viena, 2023

Agradecimientos

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) desea expresar su agradecimiento a dos expertos que prestaron asistencia en especie en las tres reuniones de grupos de expertos. En especial, agradece a Vijay Rathour, socio y Jefe del Grupo de Análisis Forense Digital de Grant Thornton, y a Samir Aliyev, Director de Programas de Ciberseguridad y Protección de Datos de la Universidad de San Galo en Suiza.

El presente documento de política fue elaborado por la Dependencia de Estrategia, Planificación y Apoyo a las Actividades sobre el Terreno de la Sección de Lucha contra la Ciberdelincuencia y el Blanqueo de Dinero de la División de Tratados de la UNODC, bajo la supervisión de Glen Prichard, Jefe de la Sección de Lucha contra la Ciberdelincuencia y el Blanqueo de Dinero.

La UNODC reconoce la contribución financiera recibida del Gobierno de los Estados Unidos de América para la preparación del presente documento de política.

Redacción

Alyaksandr Malyshau

Examen y comentarios

Michiel van Dyk

Nayelly Loya Marin

Renata Delgado-Schenk

Jonathan Fishman

Producción editorial: Sección de Servicios en Inglés, Publicaciones y Biblioteca, Oficina de las Naciones Unidas en Viena.

Imágenes de la portada: © Maksim Kabakou/stock.adobe.com, releon8211/stock.adobe.com

Índice

LISTA DE FIGURAS

Resumen

En el presente análisis de amenazas y documento de política se resumen los resultados de tres reuniones de grupos de expertos que se celebraron en 2022 en África Oriental y Meridional, América Latina y el Caribe y la región de Asia y el Pacífico. Sobre la base de las investigaciones y la bibliografía más recientes, el documento ofrece enfoques prácticos que los responsables de formular políticas pueden tener en cuenta al gestionar incidentes relacionados con programas secuestradores o prepararse para ellos.

A las tres reuniones de grupos de expertos asistieron expertos de círculos académicos y del sector privado, así como representantes de 10 países de África Oriental y Meridional (Botswana, Kenya, Malawi, Mauricio, Namibia, República Unida de Tanzanía, Seychelles, Sudáfrica, Uganda y Zambia), 9 países de América del Sur y Centroamérica (Argentina, Belice, Colombia, Costa Rica, México, Panamá, Paraguay, Perú y República Dominicana) y 11 países de la región de Asia y el Pacífico (Fiji, Filipinas, Indonesia, Islas Cook, Islas Salomón, Malasia, Papua Nueva Guinea, República Democrática Popular Lao, Samoa, Tailandia y Vanuatu).

Las reuniones tenían por objetivo examinar los riesgos y beneficios de pagar rescates a quienes realizan ataques con programas secuestradores, para lo cual se trató de dar respuesta a las siguientes cuatro preguntas fundamentales:

1. ¿Deberían plantearse pagar las víctimas?
2. ¿Cómo pueden recuperar el pago las víctimas?
3. ¿Qué cooperación se necesita para facilitar la recuperación?
4. ¿Pueden las leyes y reglamentos facilitar la recuperación de los rescates pagados?

Está claro que en todo intento de dar respuesta a la amenaza que plantean los programas secuestradores es necesario tener en cuenta las políticas y medidas que se podrían aplicar para evitar que se produzca un ataque de ese tipo. Chainalysis publicó recientemente en su blog que los ingresos de los operadores de programas secuestradores habían disminuido notablemente en 2022 debido al mayor conocimiento de las medidas de seguridad, lo que demuestra que las políticas y las medidas proactivas pueden ser muy eficaces para impedir que los agentes malintencionados logren sus objetivos[1]. Por ello, en lugar de limitarse a averiguar qué respuestas podrían darse a una extorsión, es importante también tener en cuenta y aplicar medidas preventivas que podrían proteger a la víctima en primera instancia.

En el presente documento se recogen las experiencias que transmitieron los Estados Miembros representados en las reuniones de los grupos de expertos y las recomendaciones que se formularon

[1] Chainalysis, "Ransomware revenue down as more victims refuse to pay", 19 de enero de 2023. Puede consultarse en https://blog.chainalysis.com.

durante varios días de deliberaciones, con miras a señalar al lector todas las posibles cuestiones que se deben tener en cuenta en el proceso de adopción de decisiones al prepararse para un incidente relacionado con programas secuestradores o para reaccionar ante él.

En los capítulos I a IV se resumen los resultados de las tres reuniones en forma de recomendaciones detalladas dirigidas a orientar las decisiones en materia de políticas en relación con las preguntas planteadas. En el capítulo V se ofrece una perspectiva sobre un abanico más amplio de políticas que pueden guiar el proceso de adopción de decisiones en todas las etapas de un ataque con programas secuestradores y permitir a las organizaciones determinar las respuestas más eficaces.

En general, en el presente documento se subraya la importancia de desarrollar un marco regulatorio integral sobre activos virtuales como requisito previo indispensable para poder dar una respuesta eficaz a la amenaza que plantean los programas secuestradores. Es fundamental establecer directrices de política que puedan ayudar a las organizaciones a evitar y afrontar de manera eficaz los ataques con programas secuestradores. La falta de capacidades especializadas para vigilar, detectar y rastrear las transacciones de activos virtuales pone de manifiesto la necesidad de la cooperación internacional entre los gobiernos, el sector privado y la comunidad académica para combatir esta amenaza creciente a nivel mundial. Para subsanar satisfactoriamente esas carencias, es fundamental fomentar el intercambio de información y datos sobre casos existentes, las técnicas de investigación innovadoras y las soluciones eficaces, así como ejecutar programas integrales y sostenibles de fomento de la capacidad adaptados específicamente a las necesidades de los distintos Estados Miembros.

Por último, el incremento de las capacidades de los Estados Miembros en los ámbitos indicados los preparará para combatir todos los tipos de actividades delictivas que impliquen activos virtuales, tanto en el presente como en el futuro. La creación de estructuras de gobierno eficaces y de un marco regulatorio en ese ámbito contribuirá no solo al desarrollo de economías digitales seguras, sino también a la mejora del bienestar y la seguridad financiera de las sociedades. Tales iniciativas ayudarán a fomentar la confianza en las economías digitales y a promover el uso seguro de activos virtuales, contribuyendo así a la prosperidad a largo plazo de las personas y las comunidades.

El presente documento no apoya ni promueve el pago de rescates y, por regla general, lo desaconseja. No obstante, analiza posibles situaciones hipotéticas en las que el pago ya se ha hecho o se está considerando por "fuerza mayor". No tiene carácter prescriptivo ni pretende imponer ningún punto de vista a los Estados Miembros. Por el contrario, su finalidad es informar y orientar a los responsables de formular políticas sobre cómo hacer frente a los incidentes relacionados con programas secuestradores. En última instancia, corresponde a cada jurisdicción determinar cuál es el mejor modo de proceder en el marco de su sistema nacional.

CAPÍTULO I.

¿Deberían plantearse pagar las víctimas?

Antes de responder a esta pregunta, es importante definir el término "víctima" en el contexto del presente documento. Una víctima de un ataque con programas secuestradores es una persona, organización u organismo estatal cuyo equipo, sistemas o infraestructuras de tecnologías de la información han sido atacados y resultado afectados por programas maliciosos conocidos como programas secuestradores.

El consejo generalmente aceptado para los afectados por un programa secuestrador, según se obtiene de una rápida búsqueda en Internet, es el siguiente: "No pague el rescate".

Aunque ningún Estado se ha pronunciado de manera definitiva sobre los pagos de rescate, debido en gran medida a la complejidad y la imprevisibilidad inherentes a cada caso concreto, algunos Estados Miembros indican directamente que no se debe pagar rescates[2]. Por ejemplo, en los Estados Unidos de América, el Equipo de Tareas Conjunto sobre Programas Secuestradores, compuesto por la Agencia de Seguridad de Infraestructura y Ciberseguridad, la Agencia de Seguridad Nacional, el Buró Federal de Investigaciones y el Centro Pluriestatal de Intercambio y Análisis de Información, no recomienda pagar rescates y, además, advierte de que hacerlo puede acarrear riesgos de sanciones[3]. Otros desaconsejan enérgicamente el pago y no consienten el pago a ciberdelincuentes.

En resumidas cuentas, las víctimas de programas secuestradores podrían plantearse pagar el rescate para recuperar los datos a los que han perdido acceso si un análisis exhaustivo del incidente ha demostrado lo siguiente:

- No hay posibilidad de recuperar los datos (es decir, no existen copias de seguridad o solo existen copias de seguridad infectadas).

[2] Equipo de Tareas Conjunto sobre Programas Secuestradores, "#StopRansomware Guide", mayo de 2023. Puede consultarse en www.cisa.gov.

[3] Departamento del Tesoro de los Estados Unidos, Oficina de Control de Activos Extranjeros, memorando de 21 de septiembre de 2021 titulado "Updated advisory on potential sanctions risks for facilitating ransomware payments". Puede consultarse en https://ofac.treasury.gov.

- No se conoce la existencia de herramientas de descifrado para esa cepa concreta de programa secuestrador.
- El costo y el impacto (financieros o de otro tipo) de volver a crear los datos desde cero superan de forma prohibitiva el importe del rescate exigido, o bien los daños o perjuicios adicionales previstos son inaceptables.
- Y lo que es más importante, el operador del programa secuestrador ha demostrado su capacidad de descifrar los datos, proporcionando la clave (o claves) de descifrado para una muestra razonablemente grande de los datos cifrados.

Aunque es posible que las condiciones mencionadas parezcan razonables y sencillas, hay varios aspectos complejos que es preciso analizar y definir.

No obstante, esto no es más que un punto de partida para quien se enfrente a esta amenaza. La forma concreta en que una víctima de programas secuestradores elija proceder dependerá de numerosos factores y posibles riesgos, que se analizan más detalladamente en el presente capítulo y los siguientes.

PROGRAMAS SECUESTRADORES Y ACTIVOS VIRTUALES

Quienes utilizan programas secuestradores suelen exigir el pago en forma de activos virtuales, ya que estos ofrecen un alto nivel de confidencialidad y son difíciles de rastrear. Aunque algunas cepas de programas secuestradores aceptan o presuntamente aceptan pagos de rescate en XRP (Ripple)[a] y éter[b], el bitcóin sigue siendo la criptomoneda más utilizada en ese tipo de ataques. Las criptomonedas, como el bitcóin, el éter y el XRP, tienen carácter seudónimo, lo que significa que no ofrecen información sobre la identidad de las partes que intervienen en la transacción. Monero, una criptomoneda con un alto nivel de anonimato que utiliza diversas tecnologías para ocultar las transacciones e impedir la identificación de los usuarios, ha ganado popularidad en los últimos años entre los operadores de programas secuestradores. A diferencia del bitcóin y otras criptomonedas alternativas (altcoines) que cuentan con cadenas de bloques públicas y transparentes que permiten rastrear las transacciones, las transacciones en moneros no se pueden rastrear sin disponer de claves criptográficas adicionales, lo que dificulta a los investigadores de cadenas de bloques la identificación del destinatario de un pago.

[a] Pete Evans, "Hackers threaten to reveal personal data of 90,000 Canadians caught in bank hack", CBC News, 29 de mayo de 2018. Puede consultarse en www.cbc.ca.

[b] L. Abrams, "HC7 planetary ransomware may be the first to accept Ethereum", Bleeping Computer, 9 de enero de 2018. Puede consultarse en www.bleepingcomputer.com.

Riesgos inmateriales asociados al pago del rescate

Entre los riesgos inmateriales que siempre se deberían tener en cuenta como razones de peso en contra del pago del rescate y que se deben evaluar en cada caso concreto se incluyen los siguientes:

- incentivar la delincuencia, desde el enriquecimiento ilícito hasta la financiación de la delincuencia organizada transnacional y el terrorismo;
- cuestiones de legalidad y cumplimiento asociadas a los pagos de rescate;

- probabilidad de recuperar los datos y posibilidad de una extorsión continua (doble, triple, etc.);
- daño a la reputación o daño político.

En un contexto carente de regulación, los riesgos señalados son muy particulares y subjetivos para cada víctima. Podrían verse contrarrestados por otros factores que vienen determinados, en la mayoría de los casos, por circunstancias como la actividad económica principal de la víctima, la sensibilidad de los datos sustraídos o las posibles repercusiones para los derechos de terceros. Un ejemplo de esto último sería un caso en el que una organización responsable del mantenimiento de infraestructuras críticas fuera atacada con un programa secuestrador, lo que dejaría fuera de servicio esas infraestructuras y, por ende, pondría en peligro vidas humanas.

Cuando el pago no es posible

Para pensar en realizar el pago del rescate es necesario disponer de los fondos que se exigen a cambio de los datos cifrados. Si no se dispone de fondos o no hay forma de ponerlos a disposición de la víctima, no hay nada más que debatir. Cuando la víctima es un Estado, la autorización legal para transferir fondos con este fin podría plantear una dificultad añadida si se produjera una situación de fuerza mayor que exigiera el pago, por ejemplo, en caso de que hubiera un riesgo cierto de pérdida o afectación grave de vidas humanas. Se trataría de un caso excepcional en el que ni siquiera sería viable intentar negociar el importe del rescate. En esos casos, las víctimas deberían optar, en primer lugar, o bien por buscar ayuda para recuperar los datos cifrados utilizando recursos públicos disponibles (por ejemplo, un equipo de respuesta a emergencias informáticas (EREI) o un equipo de respuesta a incidentes de seguridad informática de carácter nacional, la red del Forum of Incident Response and Security Teams (FIRST)[4] o el proyecto No More Ransom[5]), o bien por intentar recuperar y reconstruir los datos desde cero.

Prohibición legal explícita del pago del rescate

Otro aspecto importante que se debe tener en cuenta es la legalidad del pago del rescate. Aunque puede que haya varios argumentos razonables a favor de pagar el rescate en determinadas circunstancias, hacerlo podría ser sencillamente imposible o constituir una violación directa de la legislación nacional por parte de las personas responsables de tomar o ejecutar esa decisión, con todas las consecuencias jurídicas que ello supondría. Además, pagar el rescate podría acarrear también sanciones de las autoridades competentes debido a la posible violación de la normativa de protección de datos.

Los países cuya legislación prohíbe expresamente el pago de rescates a extorsionistas podrían estudiar vías jurídicas que permitan hacer excepciones en determinados casos si la víctima puede demostrar de forma justificada que el pago del rescate es la única solución práctica. Un ejemplo de ese tipo de caso sería que no hubiera forma de recuperar o reconstruir datos esenciales o que

[4] La red FIRST es una asociación mundial sin ánimo de lucro que está compuesta por equipos de respuesta a incidentes de seguridad informática y profesionales de la seguridad de todo el mundo. Su principal cometido es facilitar que los equipos de respuesta a incidentes respondan de manera más eficaz a los incidentes de seguridad y prevenir y mitigar las ciberamenazas (https://first.org).

[5] El proyecto No More Ransom es una iniciativa de la Unidad Nacional contra la Delincuencia de Alta Tecnología de la Policía de los Países Bajos, el Centro Europeo contra la Ciberdelincuencia, Kaspersky y McAfee, cuyo objetivo es ayudar a las víctimas de los ataques con programas secuestradores a recuperar sus datos cifrados sin tener que pagar a los delincuentes (www.nomoreransom.org).

hacerlo acarreara costos prohibitivos o un grave riesgo para las vidas humanas, y que el atacante que utilizara el programa secuestrador pudiera demostrar su capacidad para descifrar una muestra de los datos, con el consiguiente aumento de las posibilidades de recuperación. Si bien el presente documento no aboga por el pago de rescates, en una situación de ese tipo es fundamental que las víctimas denuncien los incidentes relacionados con programas secuestradores y cooperen estrechamente con los organismos nacionales encargados de hacer cumplir la ley, sus propios asesores jurídicos, las organizaciones internacionales pertinentes y otros asociados en las labores de planificación y ejecución de las operaciones de rastreo y recuperación de los rescates pagados.

Demostración de la capacidad de descifrar y recuperar datos

Incluso si se paga el rescate, no hay garantías de que los datos cifrados realmente se vayan a descifrar utilizando la clave facilitada por el operador del programa secuestrador. Por tanto, en los casos en que la víctima contemple pagar un rescate debido a la gravedad del riesgo evaluado, al negociar el importe y las condiciones del rescate es aconsejable pedir al operador del programa secuestrador que demuestre su capacidad de descifrar los datos, proporcionando las claves de descifrado para una muestra de los archivos. Aunque normalmente se supone que todos los datos se han cifrado utilizando el mismo algoritmo, lo ideal es confirmar la posibilidad de recobrar los archivos que son fundamentales para una recuperación rápida.

Si bien la probabilidad de recibir del atacante que utiliza el programa secuestrador una clave de descifrado o cualquier herramienta para recuperar los datos es un factor crucial para determinar si se debe pagar el rescate, esto podría no ser posible si el operador del programa secuestrador se niega a comunicarse o negociar. No obstante, hay que intentar entablar negociaciones.

Amenaza de extorsión continua

El reiterado empleo de tácticas de extorsión, conocido a menudo como doble y triple extorsión, se ha vuelto cada vez más frecuente desde 2019. Los atacantes que utilizan esas tácticas sustraen los datos realizando un reconocimiento de la red en el sistema de la víctima para determinar cuáles son los activos valiosos y transfiriéndolos a sus propias redes de almacenamiento antes de cifrar los datos. A continuación, aumentan la presión sobre la víctima para que pague el rescate, amenazándola con vender o difundir los datos en línea o con atacar a sus clientes o asociados. En esos casos, se aconseja a las víctimas que den por sentado que los datos sensibles se acabarán publicando tarde o temprano, incluso si se paga el rescate, y que adopten medidas para minimizar los daños.

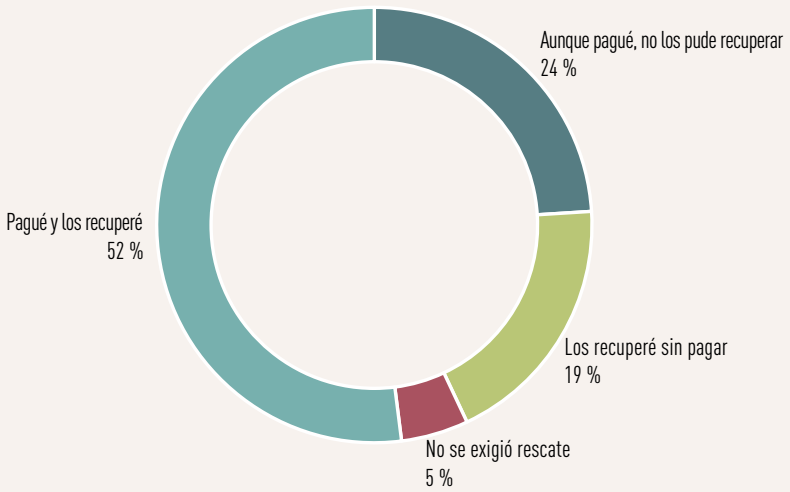
En general, es crucial que las víctimas de programas secuestradores subsanen las vulnerabilidades de ciberseguridad que posibilitaron el ataque original, evitando así ser víctimas de ataques reiterados resultantes de las mismas debilidades. Los casos documentados de doble o triple extorsión ponen de manifiesto que, si esas vulnerabilidades persisten, la negociación de pagos de rescate podría dejar de ser una opción viable.

Ventajas percibidas de pagar el rescate

Indudablemente, desembolsar una gran suma de dinero solo para recuperar datos robados no tiene nada de ventajoso; además, la recuperación en sí no es un proceso instantáneo, y garantizar que los sistemas recuperados estén limpios y sean seguros cuesta tiempo y dinero. En esta sección se analizan algunos aspectos que podrían presentarse durante un incidente relacionado con programas secuestradores y ser percibidos por las víctimas como ventajosos en una situación tal.

Por paradójico que parezca, debido a la rastreabilidad de las criptomonedas exigidas habitualmente, el pago del rescate podría ayudar a la investigación de los organismos encargados de hacer cumplir la ley y a la recuperación de fondos.

FIGURA I. RESPUESTAS A LA PREGUNTA DE LA ENCUESTA: "¿CONSIGUIÓ USTED RECUPERAR LOS DATOS DESPUÉS DE PAGAR EL RESCATE?"



Según una encuesta realizada en 2022 por una empresa de investigación independiente a 1.000 líderes del sector de la tecnología de la información[6], el 52 % de las personas encuestadas indicaron que habían recuperado sus datos después de pagar el rescate, mientras que el 24 % de las que habían pagado el rescate no habían podido recuperar sus datos (véase la figura I). Hay una probabilidad más o menos razonable de recuperar los datos cifrados, lo cual, por sí mismo, ya constituye un hecho positivo, especialmente en casos muy destacados de víctimas que explotan infraestructuras críticas o cuando un análisis del impacto en las operaciones confirma que es menos costoso pagar el rescate que reconstruir los datos. Si bien es imposible garantizar la recuperación completa o incluso parcial de los datos, es bastante más probable que sí se produzca, ya que el principal motivo que impulsa a los grupos que emplean programas secuestradores es la obtención de beneficios económicos. El incumplimiento de sus promesas repercutiría negativamente en sus ingresos ilícitos. No obstante, las estadísticas que figuran en

[6]Veeam Software, *2022 Ransomware Trends Report*. Puede consultarse en https://go.veeam.com.

el informe mencionado muestran que el pago del rescate no garantiza la recuperación de datos cifrados por un programa secuestrador.

Otra ventaja que a menudo se percibe como asociada al pago del rescate, en función de la naturaleza de los datos que se hayan cifrado, es la posible reducción de la probabilidad de que los datos se vendan o distribuyan a través de Internet. Las víctimas podrían considerar que esto sería una forma de evitar infracciones de las leyes sobre la seguridad de los datos, controlar la interrupción de sus operaciones y minimizar el daño a su reputación. Sin embargo, esa percepción es equivocada y peligrosa, ya que, como se indica en la sección relativa a la amenaza de extorsión continua, las víctimas deberían dar por sentado que los datos sensibles ya se han extraído y actuar como si se fueran a vender o hacer públicos de otra manera.

Como ya se ha indicado, si se efectúan pagos, existirá la posibilidad de investigar el delito mediante el rastreo de las transacciones de criptomonedas a fin de averiguar la identidad de los atacantes que emplearon el programa secuestrador y recuperar los fondos. Dado que estos delitos no suelen entender de fronteras, es esencial que las víctimas denuncien los incidentes a las fuerzas del orden y que las autoridades competentes empleen todos los medios disponibles, incluidos los cauces establecidos por los organismos internacionales encargados de hacer cumplir la ley. La coordinación con las autoridades encargadas de hacer cumplir la ley y las entidades del sector privado, como proveedores de servicios de activos virtuales (PSAV) y empresas de análisis de la cadena de bloques, durante la investigación de los pagos de rescate puede arrojar pistas valiosas para las investigaciones. El examen minucioso de las comunicaciones intercambiadas durante las negociaciones del rescate y después del pago también puede ser pertinente para los investigadores, ya que estas pueden aportar información valiosa sobre los atacantes y sus métodos.

Por último, aunque pagar el rescate pueda tener repercusiones negativas para las víctimas en cuanto a pérdidas financieras y deterioro de la reputación, podría impulsarlas a mejorar sus sistemas, políticas y estrategias de seguridad internos. Al descubrir las fortalezas y debilidades de su propia infraestructura de red, sus medidas de ciberseguridad y resiliencia y sus políticas de respuesta a incidentes, así como de sus políticas de creación de capacidad, formación y concienciación del personal, una organización puede aplicar los cambios necesarios en diversos niveles para mejorar sus defensas frente a futuros ataques con programas secuestradores. Las víctimas de programas secuestradores que no pagaron rescate, ya fuera por cumplir los requisitos jurídicos, debido a la falta de fondos o por contar con un plan eficaz de respuesta a incidentes que facilitara la recuperación de los datos, también pueden aprender de la experiencia.

CAPÍTULO II.

¿Cómo pueden recuperar el pago las víctimas?

La gestión de los incidentes relacionados con programas secuestradores suele verse como una ponderación de los costos y los beneficios por parte del atacante y la víctima. Para el atacante, el costo de realizar el ataque es relativamente bajo, mientras que los beneficios pueden ser sustanciosos. Por lo que respecta a las víctimas, aunque pagar el rescate pueda ser costoso, muchas están dispuestas a asumir el costo porque consideran que esto les compensa: tal vez crean que las repercusiones de no pagar puedan ser más importantes que el gasto que supone hacer el pago. Sin embargo, las víctimas que sí pagan podrían estar fomentando involuntariamente que se produjeran más ataques con programas secuestradores en lo sucesivo, ya que estarían demostrando a los atacantes que usan esos programas que sus actividades son rentables. A fin de minimizar el número de incidentes relacionados con programas secuestradores y evitar que se produzcan, es primordial que las organizaciones fomenten una cultura de la seguridad para defenderse frente a los ataques con programas secuestradores y denunciar ese tipo de incidentes ante las fuerzas del orden u otras autoridades pertinentes de manera oportuna.

Para aumentar las posibilidades de recuperar los rescates pagados en criptomonedas, es importante que las víctimas sean proactivas y estén preparadas para reaccionar de forma rápida y eficiente. Eso implica, entre otras cosas, invertir en infraestructura de ciberseguridad y notificar a las autoridades encargadas de hacer cumplir la ley tan pronto como se produzca un incidente relacionado con programas secuestradores para que determinen las direcciones de criptomonedas pertinentes y congelen las cuentas en los PSAV según sea necesario. Incluso si una organización está debidamente preparada para un ataque con programas secuestradores, es importante adoptar esas medidas cuanto antes para aumentar las posibilidades de éxito en la recuperación del rescate.

Notificación de incidentes

Cuando se produce un ataque con programas secuestradores, es esencial cumplir lo dispuesto en la legislación. Es posible que en algunas jurisdicciones sea obligatorio informar a las fuerzas del orden y otras autoridades pertinentes en un plazo concreto[7]. Además, si la víctima dispone de un seguro contra riesgos cibernéticos que cubra los incidentes relacionados con programas secuestradores, se deberán seguir los procedimientos jurídicos correspondientes. Es importante que las víctimas se pongan en contacto lo antes posible con las autoridades nacionales encargadas de hacer cumplir la ley y que informen al EREI o equipo de respuesta a incidentes de seguridad informática (de haberlos). Los organismos encargados de hacer cumplir la ley pueden iniciar las investigaciones y recibir ayuda de asociados internacionales, instituciones financieras, PSAV y empresas de análisis de la cadena de bloques. También es importante que las instituciones financieras presenten los informes necesarios si detectan transacciones sospechosas que podrían estar vinculadas a pagos de rescate o al blanqueo de dinero conexo.

Recopilación de información

La recopilación de información sobre el ataque con programas secuestradores y el atacante es un elemento crucial de la gestión del incidente, que implica, entre otras cosas, obtener detalles acerca de la dirección o direcciones de los monederos de activos virtuales en los que se ha exigido que se efectúe el pago, así como analizar el tráfico de la red antes del ataque. El organismo encargado de hacer cumplir la ley pertinente debería examinar exhaustivamente las comunicaciones entre la víctima, sus sistemas y el atacante, en busca de cualquier información útil que pudiera resultar de ayuda para la investigación. Recopilando tanta información como sea posible de todas las fuentes disponibles, se acrecientan las probabilidades de obtener un resultado favorable para la víctima. Además de las acciones emprendidas por los organismos encargados de hacer cumplir la ley para dar respuesta a la actividad delictiva, los EREI o los equipos de respuesta a incidentes de seguridad informática (de haberlos) desempeñan sus propias funciones cruciales. Estos equipos son responsables de recopilar y analizar los datos y las tendencias relacionados con la ciberseguridad. Su cometido consiste en detectar posibles amenazas y vulnerabilidades y desarrollar estrategias y políticas eficaces para contrarrestarlas.

Casos de fuerza mayor que afectan a vidas humanas

En los casos de fuerza mayor en que las pérdidas y repercusiones previstas de un ataque con programas secuestradores superen los niveles de daño aceptables (a menudo en situaciones que tienen consecuencias negativas para las vidas humanas), la negociación de pagos de rescate podría convertirse en una opción viable para evitar pérdidas de mayor importancia.

En esos casos, recurrir a los servicios de una empresa especializada en ciberseguridad con amplios conocimientos en materia de negociación y recuperación de rescates podría resultar ventajoso incluso si la organización afectada dispone de especialistas propios. La experiencia de los

[7] Los requisitos de notificación de incidentes relacionados con programas secuestradores o filtraciones de datos varían de una jurisdicción a otra. Los plazos de notificación pueden ir desde dos horas hasta 60 días a partir del descubrimiento del incidente, dependiendo del tipo de actividad económica de la víctima y la sensibilidad de los datos. En la formulación de los requisitos suelen aparecer expresiones como "lo antes posible", "tan pronto como sea factible" o "tan pronto como sea posible".

negociadores especializados puede ser de gran ayuda para reducir el importe del rescate, minimizar las repercusiones del ataque y recopilar pruebas útiles para identificar a los delincuentes[8].

Se recomienda incluir una o varias empresas especializadas en ciberseguridad, verificadas previamente, en el plan de mitigación de ataques con programas secuestradores. En ausencia de tales disposiciones, es posible que las fuerzas del orden y los asociados internacionales puedan proporcionar referencias fiables.

En los casos en que se contempla la posibilidad de pagar el rescate, se recomienda hacerlo en una criptomoneda que esté basada en una cadena de bloques pública y transparente, de modo que se puedan rastrear todas las direcciones implicadas en la transacción. El bitcóin, que se usa con frecuencia para los pagos de rescate, y otras criptomonedas alternativas, como el éter, el litecoin y el XRP, funcionan sobre la base de cadenas de bloques públicas. Sin embargo, cada vez más operadores de programas secuestradores exigen el pago en moneros, una criptomoneda con un mayor nivel de anonimato. Se recomienda negociar que el pago se haga en bitcoines u otra criptomoneda que se pueda rastrear, incluso si los atacantes exigen un importe menor en moneros u otra criptomoneda con un mayor nivel de anonimato. Los delincuentes son conscientes de que determinadas criptomonedas se pueden rastrear y podrían elevar el importe del rescate para compensar el costo de las actividades adicionales de ocultación de fondos.

Notificar a las fuerzas del orden los incidentes relacionados con programas secuestradores puede hacer que aumenten considerablemente las posibilidades de recuperar los rescates pagados, ya que conduce a una mejor cooperación y coordinación con los PSAV, tanto a nivel nacional como internacional. Esa cooperación podría reportar a las víctimas una ventaja estratégica sobre los atacantes y posibilitar el bloqueo y la congelación de los fondos cuando se transfieran a una plataforma centralizada de cambio de criptomonedas.

[8] Pepijn Hack y Zong-Yu Wu, "We wait, because we know you: inside the ransomware negotiation economics", publicado por Aaron Haymore, NCC Group Research, el 12 de noviembre de 2021. Puede consultarse en https://research.nccgroup.com.

CAPÍTULO III.

¿Qué cooperación se necesita para facilitar la recuperación?

Para recuperar el rescate pagado, se necesita una estrecha colaboración entre todas las partes interesadas, incluidos los gobiernos, las empresas privadas y los ciudadanos. Las empresas especializadas en ciberseguridad y análisis de la cadena de bloques pueden ofrecer sus conocimientos especializados para ayudar a investigar el movimiento de las transacciones de activos virtuales e identificar las "vías de escape" utilizadas por los delincuentes para convertir en efectivo sus ganancias. Al tiempo que las fuerzas del orden y los fiscales investigan los ataques con programas secuestradores y enjuician a sus autores, las instituciones financieras pueden desempeñar un papel importante detectando y notificando actividades sospechosas que podrían estar vinculadas a ciberataques, como los realizados con programas secuestradores, mediante la detección, la notificación y el bloqueo de pagos de rescate. También pueden ayudar a las víctimas a recuperar sus fondos, a menudo con el apoyo de las fuerzas del orden.

Sensibilización y educación

Para combatir de manera eficaz la delincuencia relacionada con los programas secuestradores, es fundamental reforzar la sensibilización y la educación del público en relación con varios aspectos clave, como el modo en que los delincuentes que usan programas secuestradores seleccionan y victimizan a las organizaciones, las maneras en que las organizaciones pueden protegerse contra los ataques con programas secuestradores, la importancia de notificar los ataques cuando se producen y las mejores prácticas que se deben seguir para responder a un ataque con programas secuestradores. Esas iniciativas son beneficiosas no solo para los organismos encargados de hacer cumplir la ley, sino también para la sociedad en su conjunto. Si se realizan campañas educativas e iniciativas de sensibilización, el público puede llegar a comprender mejor este delito y cómo reaccionar ante él de manera eficaz.

Esas campañas e iniciativas pueden llevarse a cabo a través de diversos medios de comunicación, como anuncios impresos, mensajes de interés público y otras formas de difusión. Además, se puede alentar a escuelas y organizaciones comunitarias a dar charlas informativas sobre el tema. Con una adecuada comprensión, todo el mundo puede ser más consciente de la amenaza que

suponen los programas secuestradores y cómo detectarla. Esto podría conducir a una mejor notificación del delito y a respuestas más eficaces, y contribuir en última instancia a reducir la prevalencia del delito.

Cooperación interinstitucional a nivel nacional

La cooperación interinstitucional a nivel nacional es vital para lograr la recuperación de los rescates pagados. En ausencia de colaboración entre distintos organismos públicos, las complejidades de este tipo de ciberdelincuencia pueden ser difíciles de desentrañar y tal vez no se disponga de los recursos necesarios.

La colaboración de las fuerzas del orden y las fiscalías, los organismos de reglamentación financiera, las agencias de inteligencia y los EREI o equipos de respuesta a incidentes de seguridad informática de nivel nacional les permite compartir recursos, como personal especializado, análisis, investigaciones e información de inteligencia sobre las actividades de grupos delictivos. Ese tipo de colaboración puede ayudar a determinar el origen del programa secuestrador, el mecanismo de pago y el esquema de los flujos de transacciones. Esto es importante para ayudar a las víctimas a recuperar sus fondos, así como para identificar a los delincuentes y proporcionar pruebas para el enjuiciamiento penal. Los organismos mencionados deberían colaborar para simplificar el marco regulatorio aplicable a la recuperación de los rescates pagados.

Un aspecto clave de la cooperación interinstitucional a nivel nacional es la participación de los organismos encargados de hacer cumplir la ley, que pueden ayudar a localizar a los atacantes y recopilar pruebas para el enjuiciamiento penal. Con sus recursos y conocimientos especializados, esos organismos pueden desempeñar un papel decisivo en la interrupción de las actividades de los operadores de programas secuestradores y la prevención de futuros ataques.

Otro aspecto importante de la cooperación interinstitucional a nivel nacional es la capacidad de detectar rápidamente la existencia de casos de programas secuestradores relacionados entre sí y la posibilidad de vincular a los delincuentes que están detrás de ellos, así como de identificar a las víctimas de los ataques y prestarles asistencia. Esa asistencia podría consistir en proporcionar recursos a las víctimas para ayudarlas a recuperar sus datos y ofrecerles asesoramiento sobre cómo prevenir futuros ataques. También puede ayudar a que se recuperen adecuadamente los pagos efectuados a los atacantes y que los fondos recuperados se destinen a apoyar a las víctimas de ataques.

En el caso de los ataques con programas secuestradores, los EREI y los equipos de respuesta a incidentes de seguridad informática (si se han establecido) suelen estar bien equipados para proporcionar apoyo crítico en materia de ciberseguridad a organizaciones que se han visto afectadas. No solo pueden proporcionar asesoramiento técnico sobre cómo mitigar el daño causado por el ataque, sino que también pueden ayudar a recuperar datos cifrados y proporcionar información a los organismos encargados de hacer cumplir la ley que investigan el incidente, cuando se solicite.

Los organismos gubernamentales pueden elaborar reglamentos y políticas para reforzar la ciberseguridad, fortalecer la prevención de la ciberdelincuencia y mejorar las medidas de resiliencia con miras a ofrecer protección frente a los ataques con programas secuestradores y ayudar a las organizaciones a recuperarse de esos incidentes. Por ejemplo, pueden imponer normas de seguridad más estrictas e informar al público de las mejores prácticas para evitar los ataques

con programas secuestradores. Esa cooperación interinstitucional puede llevar a la creación de estrategias más amplias y eficaces de lucha contra los programas secuestradores y conseguir que las organizaciones y los particulares estén mejor protegidos frente a esta amenaza creciente.

Cooperación internacional

La cooperación internacional entre organismos encargados de hacer cumplir la ley, organismos de reglamentación financiera, autoridades de recuperación de activos y empresas de ciberseguridad se considera fundamental para el éxito de las medidas encaminadas a combatir los ataques con programas secuestradores. La cooperación entre esas entidades no solo ayuda en los aspectos técnicos de recuperación de datos, sino que también posibilita una respuesta integral de la justicia penal. Facilita la investigación a nivel mundial de ciberdelitos, contribuye al enjuiciamiento de delincuentes en las distintas jurisdicciones y fomenta el intercambio de información y recursos cruciales, reforzando así la resiliencia mundial contra los ataques con programas secuestradores. Las organizaciones internacionales y las redes regionales de recuperación de activos pueden proporcionar los recursos y los conocimientos especializados necesarios para coordinar una respuesta en varios países, lo que posibilita una comunicación más eficaz en las investigaciones forenses, la obtención de pruebas y la coordinación del proceso de recuperación. Ese tipo de cooperación también puede ayudar a que se aborden correctamente todos los aspectos de los procesos de respuesta y recuperación y a que todas las partes implicadas estén plenamente informadas de la situación. Mediante la colaboración, pueden aprovecharse los conocimientos especializados de los países que cuenten con capacidades avanzadas de investigación de amenazas con programas secuestradores y rastreo de pagos de activos virtuales para apoyar a los Estados cuyas capacidades en este ámbito estén menos desarrolladas y fomentar su capacidad a este respecto.

El intercambio rápido de información de inteligencia sobre ataques con programas secuestradores entre los EREI o equipos de respuesta a incidentes de seguridad informática y los organismos encargados de hacer cumplir la ley de los Estados Miembros permite establecer vínculos entre incidentes relacionados entre sí, lo cual, a su vez, sirve de base para las iniciativas de rastreo de activos virtuales y facilita el progreso de las investigaciones. Además, esta cooperación podría ayudar a las autoridades a informar a la ciudadanía de las estrategias empleadas por los delincuentes y podría permitir a los particulares adoptar las medidas de precaución necesarias y evitar convertirse en víctimas de esos ataques.

Colaboración o cooperación público-privada

Las alianzas público-privadas oficiales ofrecen un marco para la colaboración y el intercambio de información entre organizaciones del sector privado y organismos públicos. Por ejemplo, las instituciones financieras, como los bancos y los PSAV, pueden vigilar las transacciones y detectar pagos de rescate y, en los casos en que se dispone de una reglamentación adecuada, están obligadas a notificar a las autoridades competentes las actividades sospechosas que puedan estar relacionadas con programas secuestradores, mientras que las compañías de seguros podrían proporcionar apoyo financiero para la recuperación de rescates pagados. Las empresas de ciberseguridad y las de respuesta a incidentes pueden proporcionar información técnica sobre los métodos utilizados por los atacantes que emplean programas secuestradores, ayudar a localizar el origen de los ataques e informar a los organismos encargados de hacer cumplir la ley.

Las alianzas público-privadas oficiosas, como los acuerdos de intercambio de información, también desempeñan un papel esencial en la recuperación de los rescates. Las instituciones financieras, las compañías de seguros y las empresas de ciberseguridad pueden proporcionar información valiosa a los organismos encargados de hacer cumplir la ley, aunque no existan alianzas oficiales. Por ejemplo, las empresas de ciberseguridad pueden aportar información sobre los métodos empleados por los atacantes que utilizan programas secuestradores, mientras que las compañías de seguros pueden proporcionar orientación contrastada sobre las estrategias de recuperación más eficaces.

Combinando los recursos del sector financiero, las compañías de seguros y las empresas de ciberseguridad, es posible crear un sistema más completo y capaz de responder mejor a los singulares desafíos que plantean los programas secuestradores. Esas alianzas también permiten a los organismos encargados de hacer cumplir la ley acceder a información e inteligencia valiosas para investigar y enjuiciar a los delincuentes.

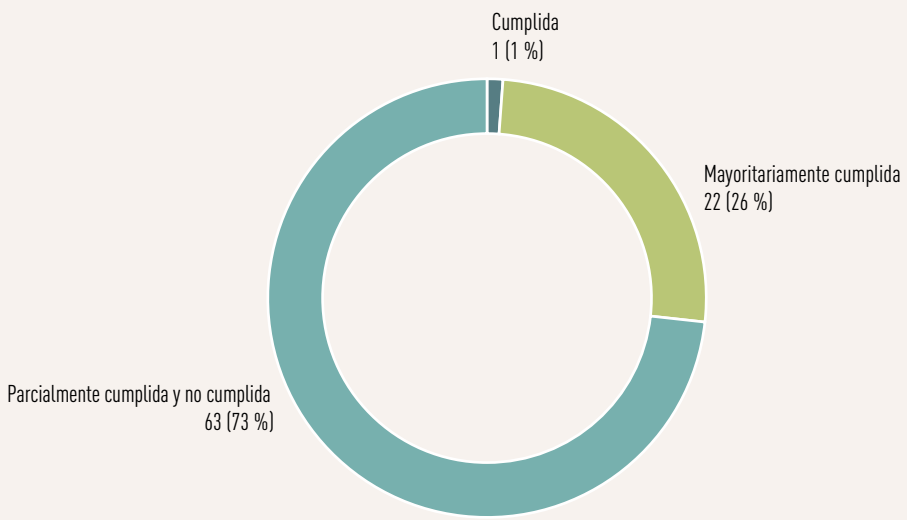
CAPÍTULO IV.

¿Pueden las leyes y reglamentos facilitar la recuperación de los rescates pagados?

Actualmente existe un vacío legal en torno al pago de rescates por ataques con programas secuestradores. En este contexto, los Estados tienen la opción de crear o modificar los marcos jurídicos y regulatorios pertinentes para hacer frente con eficacia a la cuestión de los pagos de rescate, aplicando las normas internacionales de lucha contra el blanqueo de dinero y la financiación del terrorismo relativas a activos virtuales y PSAV, y haciendo que los ciberdelincuentes rindan cuentas por sus actos.

Ventajas de los regímenes de lucha contra el blanqueo de dinero y la financiación del terrorismo relativos a los activos virtuales

FIGURA II. NÚMERO (Y PORCENTAJE) DE JURISDICCIONES EVALUADAS SEGÚN LA METODOLOGÍA REVISADA DE LA RECOMENDACIÓN 15



La aplicación a activos virtuales y PSAV de las normas internacionales de lucha contra el blanqueo de dinero y la financiación del terrorismo puede reducir la medida en que los delincuentes que emplean programas secuestradores utilizan activos virtuales y PSAV para blanquear sus ganancias ilícitas. Según el informe del Grupo de Acción Financiera (GAFI) sobre la lucha contra la financiación de los programas secuestradores (*Countering Ransomware Financing*), en enero de 2023, de las 86 jurisdicciones evaluadas según las normas revisadas (recomendación 15), 63 (el 73 %) incumplían parcial o totalmente esos requisitos. Solo 1 de las 86 jurisdicciones los cumplía plenamente (véase la figura II)[9]. Las recomendaciones del GAFI se aplican a los activos virtuales y los PSAV, y promueven un enfoque basado en los riesgos con respecto a las actividades y operaciones con activos virtuales y los PSAV; la supervisión o vigilancia de PSAV con fines de lucha contra el blanqueo de dinero y la financiación del terrorismo; la concesión de licencias o inscripción en registros; medidas preventivas, como la diligencia debida con respecto al cliente, el mantenimiento de registros y la notificación de las transacciones sospechosas; sanciones y otras medidas coercitivas, y la cooperación internacional. La adopción de esas medidas puede contribuir a detectar e interrumpir el blanqueo de dinero relacionado con programas secuestradores, mediante la notificación por parte de las instituciones financieras de las transacciones sospechosas que puedan estar relacionadas con programas secuestradores, a través de la recopilación de información por parte de las instituciones financieras que pueda servir de base a las investigaciones de las fuerzas del orden, y mediante la existencia de mecanismos de coordinación entre las autoridades nacionales e internacionales, por dar solo algunos ejemplos.

Normas eficaces en relación con las infraestructuras críticas

Se aconseja a los Estados que adopten normas que ofrezcan un marco para tomar decisiones fundamentadas en relación con los pagos de rescates y evitar que estos se conviertan en una fuente de ingresos para los ciberdelincuentes. En cuanto a los programas secuestradores en particular, las normas que regulan las medidas de las entidades que explotan infraestructuras críticas son de la máxima importancia, ya que un ataque contra ellas con programas secuestradores puede tener consecuencias trascendentales para el funcionamiento de la sociedad.

Al elaborar normas relacionadas con las infraestructuras críticas, los Estados deben evaluar cuidadosamente el nivel óptimo de control, que abarcará desde las normas operativas hasta las instrucciones administrativas. También deben elegir con buen criterio el ámbito jurídico más adecuado para regular esas normas, ya sea el derecho administrativo, el civil o el penal.

Por encima de todo, es imperativo que esas normas sean inequívocas y aplicables, y que incluyan un requisito obligatorio de notificación a los organismos normativos y organismos encargados de hacer cumplir la ley pertinentes. Esto garantizará no solo el cumplimiento, sino también la seguridad y la resiliencia de las infraestructuras críticas del Estado. No obstante, el elemento más importante es disponer de medidas adecuadas para prevenir futuros ataques y reducir el riesgo de que los pagos de rescate se utilicen para actividades ilegales. Es fundamental aplicar medidas de ciberseguridad exhaustivas, lo que supone realizar auditorías de seguridad periódicas, mantener actualizados los programas informáticos, aplicar políticas sobre el uso de contraseñas seguras y proporcionar capacitación a los empleados. Todas esas acciones son esenciales para responder a las ciberamenazas.

[9] Grupo de Acción Financiera (GAFI), *Countering Ransomware Financing* (París, 2023), párr. 33.

Minimizar el riesgo de apoyar actividades ilegales

Es posible que los atacantes intenten aprovecharse de los puntos débiles de los marcos regulatorios y jurídicos relativos a la ciberseguridad y la protección de datos para efectuar sus ataques con un riesgo mínimo de ser descubiertos o castigados. Las normas relativas a los programas secuestradores deberían formularse de forma que alentaran a las organizaciones a elaborar planes integrales y establecer sistemas de gestión pertinentes con arreglo a las normas de la Organización Internacional de Normalización (ISO), evitando al mismo tiempo la creación de disposiciones explícitas de las que los atacantes podrían sacar partido. Esos planes y sistemas podrían incluir un sistema de gestión de la seguridad de la información y un plan de gestión de incidentes[10], así como un plan de continuidad de las operaciones y un plan de recuperación en casos de desastre[11], y un sistema de gestión de la información de privacidad[12]. Además, las normas deberían incluir disposiciones especiales para aquellos casos que puedan considerarse financiación del terrorismo, con el fin de garantizar que las organizaciones no apoyen inadvertidamente actividades ilegales. Esas disposiciones deben redactarse cuidadosamente para garantizar que las organizaciones reciban la orientación y el apoyo necesarios para responder a los ataques con programas secuestradores que presenten esas características.

[10] Organización Internacional de Normalización, ISO/IEC 27001:2022 (octubre de 2022).

[11] ISO 22301:2019 (octubre de 2019).

[12] ISO/IEC 27701:2019 (agosto de 2019).

CAPÍTULO V.

Adopción de decisiones sobre incidentes relacionados con programas secuestradores

Mientras que los capítulos I a IV se centran en cuestiones relacionadas con las respuestas relativas a los pagos de rescate, este capítulo adopta un enfoque más integral sobre cómo hacer frente a un incidente relacionado con programas secuestradores y ofrece una visión general de todos los aspectos que intervienen en la adopción de decisiones en relación con un ataque con programas secuestradores, desde las políticas de prevención hasta la investigación y el análisis posterior al incidente. El árbol de decisión que se muestra en la figura III representa las principales etapas de este proceso, que se describirán en más detalle en las secciones siguientes.

Prevención

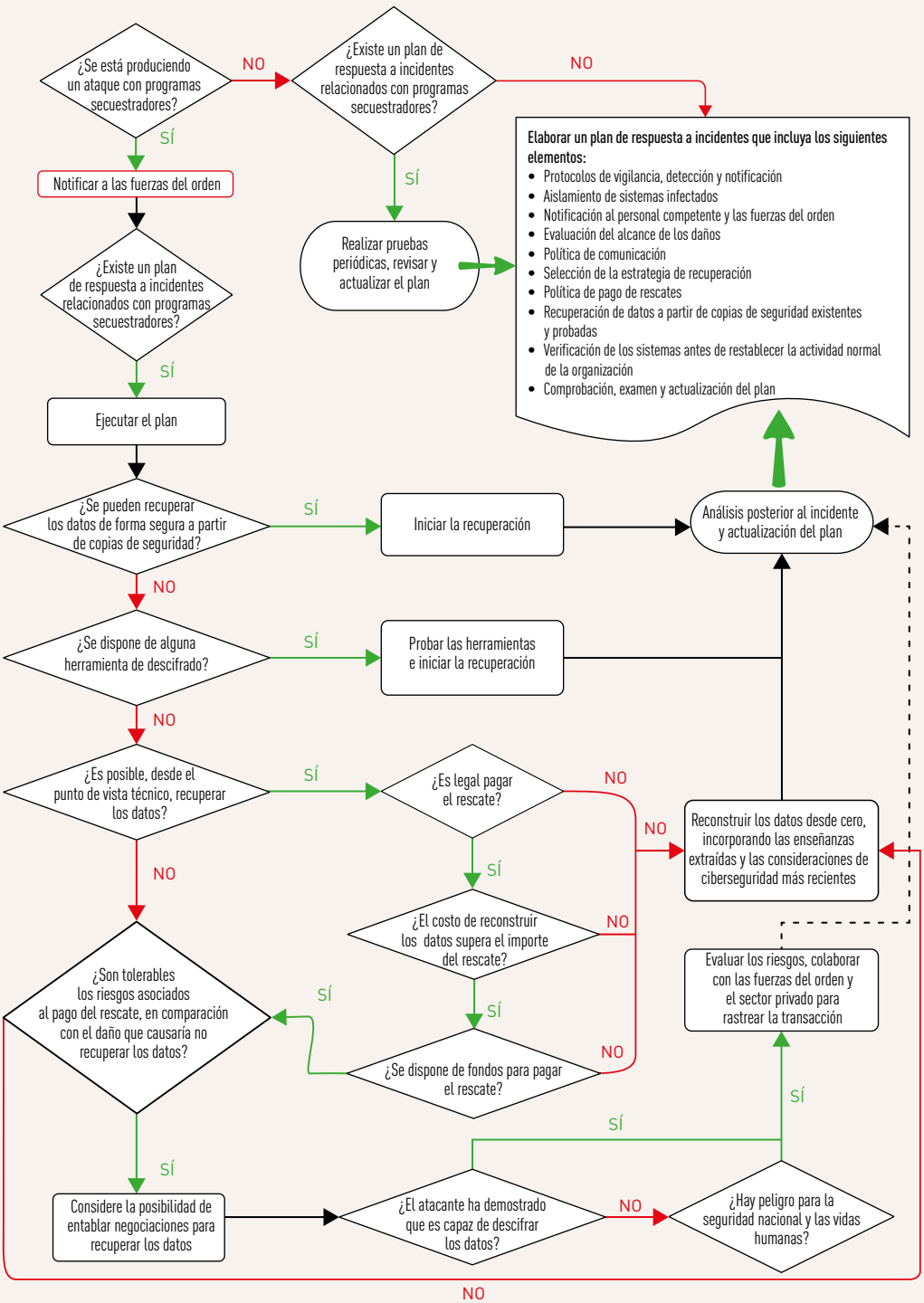
Las políticas de prevención de ataques con programas secuestradores contemplan las preguntas que se deben plantear para decidir el modo de proceder adecuado en caso de un ataque con un programa secuestrador. Si una organización aplica correctamente esas políticas, las probabilidades de recuperar los datos perdidos sin necesidad de pagar un rescate a los atacantes pueden ser muy elevadas. Las políticas se refieren principalmente a temas que ya se han mencionado en el presente documento, como las copias de seguridad de los datos, las estrategias y políticas de ciberseguridad, la educación y la formación sobre ciberdelincuencia —con especial énfasis en los programas secuestradores— y los seguros contra riesgos cibernéticos, si procede.

Educación y sensibilización

Las políticas de educación y sensibilización desempeñan un papel fundamental en la prevención de ataques con programas secuestradores a nivel de las organizaciones. Para tal fin, las organizaciones podrían considerar la aplicación de las siguientes políticas:

- Formación para la sensibilización en materia de seguridad. Proporcionar formación para la sensibilización sobre seguridad a todos los empleados, que incluya información sobre cómo detectar y evitar estafas de suplantación de identidad, ataques de suplantación de identidad dirigidos contra la organización y mejores prácticas para la gestión segura de los datos.

FIGURA III. PROCESO DE ADOPCIÓN DE DECISIONES EN RESPUESTA A UN ATAQUE CON PROGRAMAS SECUESTRADORES



- Formación en materia de respuesta a incidentes. Impartir formación periódica sobre respuesta a incidentes para que los empleados estén preparados para reaccionar de manera eficaz frente a un ataque con programas secuestradores, sepan qué medidas deben adoptar y comprendan claramente sus funciones y responsabilidades.
- Actualizaciones periódicas de la información y seguridad. Proporcionar a todos los empleados, de manera periódica, información actualizada y complementaria y mantenerlos al tanto de las últimas amenazas y vulnerabilidades.
- Formación en materia de control del acceso. Proporcionar formación a los empleados sobre las políticas de control del acceso y cómo aplicarlas para evitar accesos no autorizados a datos y sistemas sensibles.
- Formación sobre el uso de dispositivos personales. Proporcionar formación sobre las políticas y directrices sobre el uso de dispositivos personales para que los empleados sepan cómo utilizarlos para acceder de manera segura a los datos y sistemas de la organización.
- Formación en materia de cifrado. Proporcionar formación a los empleados sobre el uso de herramientas de cifrado y cómo utilizarlas para proteger los datos sensibles frente al acceso no autorizado o el robo.
- Formación en materia de seguridad de terceros. Proporcionar formación a los empleados sobre las políticas y directrices de seguridad de terceros y sobre cómo garantizar que los proveedores y prestadores de servicios externos sigan protocolos de seguridad adecuados.
- Formación en materia de notificación de incidentes. Proporcionar formación a los empleados sobre cómo notificar los incidentes de seguridad, incluidos los posibles ataques con programas secuestradores, al personal correspondiente o al departamento de tecnología de la información, y establecer cauces de notificación y procedimientos claros para esos incidentes.

Copias de seguridad y recuperación

Para superar un ataque con programas secuestradores, es fundamental disponer de una política integral sobre las copias de seguridad y la recuperación de datos. Aunque la estrategia de copias de seguridad y recuperación suele formar parte de la estrategia general de ciberseguridad, el presente documento hace hincapié en su importancia capital para protegerse frente a un ataque con programas secuestradores. En la política se deben incluir, entre otras, las siguientes consideraciones:

- Copias de seguridad. Desarrollar una estrategia de copias de seguridad que incluya copias de seguridad periódicas y automatizadas de los datos críticos, que se conserven en ubicaciones seguras en línea, fuera de línea o externas.
- Comprobaciones. Comprobar periódicamente los sistemas y procedimientos de copias de seguridad para asegurarse de que funcionen según lo previsto y puedan restablecerse rápidamente las operaciones normales en caso de ataque.
- Conservación. Elaborar una política de conservación que defina el plazo de conservación de los datos y la frecuencia con la que se harán copias de seguridad de ellos.
- Control del acceso. Controlar el acceso a los sistemas y datos de copias de seguridad para evitar el acceso no autorizado o la manipulación.

- Copias de seguridad para el plan de respuesta a incidentes. En el plan de respuesta a incidentes relacionados con programas secuestradores de la organización, incluir procedimientos específicos para responder a un ataque con programas secuestradores y recuperar los datos a partir de copias de seguridad.

Evaluación de riesgos

En la gestión de un incidente relacionado con programas secuestradores, los dos elementos clave son el grado de preparación de la organización y la gravedad percibida del ataque. La gravedad del ataque vendrá determinada por los tipos de sistemas afectados, los datos cifrados, el riesgo relativo para los intereses de seguridad nacional y las preocupaciones relativas a la privacidad de los datos. La gravedad se puede clasificar generalmente como alta, media o baja. Por su parte, el grado de preparación para un ataque con programas secuestradores se puede clasificar simplemente como alto, cuando se dispone de un plan de respuesta a incidentes y personal capacitado, o bajo, cuando no se dispone de ellos. Aunque es posible que existan grados de preparación intermedios, la organización en cuestión debería poder determinar su propio grado de preparación en cada situación. El nivel de preparación dependerá principalmente de las capacidades internas de la organización y de su comprensión de lo importante que es proteger sus datos críticos para la continuidad de las operaciones. Las organizaciones que consideran que sus datos son críticos para sus operaciones suelen aplicar planes de respuesta a incidentes y proporcionar formación a su personal para que los ejecute.

En el siguiente cuadro se resume el modo de proceder habitual en las distintas combinaciones de gravedad del ataque y grado de preparación.

MATRIZ DE DECISIÓN EN FUNCIÓN DE LA GRAVEDAD DEL ATAQUE Y EL GRADO DE PREPARACIÓN

GRADO DE PREPARACIÓN / GRAVEDAD DEL ATAQUE	ALTO Existe un plan de respuesta a incidentes, el personal está capacitado	BAJO No existe un plan de respuesta a incidentes, el personal no está capacitado
ALTA Infraestructuras críticas, seguridad pública, sistemas de seguridad nacional	Seguir el plan de respuesta a incidentes y colaborar con expertos externos según sea necesario	Buscar asistencia externa y aplicar las mejores prácticas de respuesta a incidentes
MEDIA Sistemas críticos para la organización, riesgo de pérdida de datos	Seguir el plan de respuesta a incidentes y contemplar la posibilidad de colaborar con expertos externos según sea necesario	Buscar asistencia externa y aplicar las mejores prácticas de respuesta a incidentes
BAJA No existe un riesgo inminente para las operaciones críticas ni pérdida de datos	Seguir el plan de respuesta a incidentes y realizar una investigación exhaustiva para determinar la causa fundamental del ataque	Buscar asistencia externa y aplicar las mejores prácticas de respuesta a incidentes

Notificación y documentación de incidentes

Notificar los incidentes relacionados con programas secuestradores es esencial para gestionar sus repercusiones y mitigar los posibles daños. Es fundamental contar con un plan bien definido para notificar incidentes de ese tipo a las partes interesadas internas y externas pertinentes, y seguir directrices específicas en materia de comunicación y documentación. Esas medidas pueden ayudar a proteger a la organización de daños mayores, minimizar las interrupciones de las operaciones y aumentar las probabilidades de que un análisis posterior al incidente sea de utilidad.

Los criterios para informar y notificar a las partes interesadas cuando se produce un incidente relacionado con programas secuestradores dependen de la gravedad del ataque, el tipo de datos afectados y las políticas internas de la organización. En la mayoría de los casos, los incidentes que afecten a datos sensibles o clasificados o repercutan en la seguridad nacional y en infraestructuras críticas deberían notificarse de inmediato a las autoridades pertinentes. Existen otros factores críticos que podrían hacer necesaria la notificación, como las posibles obligaciones legales o contractuales o la reglamentación específica del sector.

También se debe contar con directrices de comunicación interna para asegurar que todo el personal competente esté informado de la situación y sea consciente de sus funciones y responsabilidades. Entre ese personal debe encontrarse la alta dirección, el personal de los departamentos de tecnología de la información, jurídico y de recursos humanos y cualquier otra parte pertinente. La comunicación debe ser oportuna, precisa y sistemática, y debe incluir información actualizada sobre el estado del incidente y las medidas que se están adoptando para gestionarlo. También es esencial mantener canales de comunicación claros y asegurarse de que todas las partes entiendan los requisitos de confidencialidad de la situación.

Deberían existir directrices sobre la comunicación externa para notificar a las partes interesadas externas, como los clientes, los proveedores y los asociados. Las organizaciones deberían dirigirse a las partes interesadas de manera clara y transparente, y proporcionarles información exacta y actualizada sobre el incidente y las medidas que se están adoptando para hacerle frente. La comunicación debería ser específica y adecuada a los destinatarios, y podría servirse de varios canales, como el correo electrónico, los medios sociales y los comunicados de prensa.

Documentar todos los procesos y procedimientos es esencial para que el análisis posterior al incidente sea de utilidad. La documentación debería incluir toda la información pertinente, como la cronología de los hechos, las medidas adoptadas para hacer frente al incidente y los registros de las comunicaciones. Debería ser exhaustiva y precisa y conservarse en una ubicación segura para su futura consulta.

Ciberseguridad

Dada la prevalencia generalizada de los programas secuestradores, es de suma importancia implementar una estrategia de seguridad que abarque toda la organización. Con independencia de la sensibilidad o el valor de sus datos, todas las organizaciones, sea cual sea su tamaño, deberían aplicar un conjunto adecuado de políticas para salvaguardar sus intereses. Si bien las organizaciones que son críticas para el funcionamiento normal de la sociedad deben estar obligadas por ley a aplicar medidas de ese tipo, otros tipos de organizaciones podrían decidir hacerlo sobre la base de sus objetivos comerciales y por razones de mercado.

Entre las políticas de ciberseguridad que pueden adoptar las organizaciones para ayudar a prevenir ataques con programas secuestradores, se encuentran las siguientes[13]:

- Respuesta a incidentes. Elaborar una política de respuesta a incidentes en la que se enuncien las medidas que se deben adoptar en caso de que se produzca un ataque con programas secuestradores. Esa política debería especificar las funciones y responsabilidades de cada miembro del equipo de respuesta a incidentes e incluir procedimientos de comunicación, cadenas de notificación a instancias superiores y procedimientos para notificar a las fuerzas del orden, los clientes y los proveedores.
- Actualizaciones periódicas. Aplicar una política de actualizaciones periódicas para que todos los programas y los equipos informáticos, incluidos los sistemas operativos, las aplicaciones y los programas informáticos de seguridad, reciban oportunamente actualizaciones y parches para subsanar vulnerabilidades conocidas.
- Segmentación de redes. Segmentar la red de la empresa para reducir las repercusiones de un ataque y asegurar que los datos de las copias de seguridad no se vean comprometidos. Esta política debería especificar cómo es el flujo de datos a través de la red, quién puede acceder a cada segmento y cómo se transmiten los datos entre segmentos.
- Control del acceso. Aplicar una política de control del acceso que restrinja el acceso a los datos y sistemas sensibles a los usuarios autorizados y les otorgue los privilegios mínimos necesarios para realizar su trabajo.
- Uso aceptable. Establecer una política de uso aceptable que incluya directrices sobre el uso aceptable de los sistemas, los dispositivos y las redes de la organización. En la política deberían recogerse las mejores prácticas para evitar los ataques con programas secuestradores, como no hacer clic en enlaces sospechosos y no descargar archivos adjuntos desconocidos.
- Vigilancia. Formular una política de vigilancia que especifique las herramientas y técnicas empleadas para vigilar los sistemas en busca de indicios de posibles ataques con programas secuestradores, como una actividad inusual de la red e intentos de acceso no autorizado.
- Acceso a distancia. Elaborar una política de acceso a distancia que incluya directrices sobre el acceso a los sistemas y datos de la organización desde ubicaciones lejanas y que contemple el uso de redes privadas virtuales y otros protocolos de acceso seguro.
- Seguridad de terceros. Formular una política de seguridad de terceros que describa a grandes rasgos los requisitos de seguridad para proveedores y prestadores de servicios externos. La política debería detallar los procedimientos necesarios para llevar a cabo los exámenes de la diligencia debida y controlar las prácticas de seguridad de terceros que tengan acceso a los sistemas y datos de la organización.
- Asistencia externa. Establecer relaciones con expertos externos, como equipos de respuesta a incidentes, asesores jurídicos y fuerzas del orden, para que proporcionen apoyo adicional en caso de que se produzca un ataque.

[13] Las políticas enumeradas aquí se pueden ejecutar como parte de las medidas de la organización para la aplicación de la norma ISO/IEC 27001:2022, de octubre de 2022.

Seguro contra riesgos cibernéticos

Como parte de las pólizas más generales de seguros contra riesgos cibernéticos, el seguro contra ataques con programas secuestradores está ganando popularidad a medida que las empresas se vuelven más conscientes de los riesgos que comportan esos ataques. Un seguro de ese tipo podría ser extremadamente valioso en un incidente relacionado con programas secuestradores, ya que puede proporcionar protección financiera a una organización en caso de que se produzca un ataque con programas secuestradores y cubrir los costos de los rescates, la recuperación de datos y otros gastos conexos. Además, un seguro de ese tipo suele cubrir el acceso a servicios de respuesta a incidentes, que pueden minimizar las repercusiones de un ataque, y ofrecer apoyo en materia de evaluación de riesgos, ayudando así a detectar posibles vulnerabilidades en las estrategias de ciberseguridad de la organización, que podrá adoptar medidas para reducir el riesgo de futuros ataques.

Al mismo tiempo, es prudente actuar con cautela en relación con las pólizas de seguros contra riesgos cibernéticos por ataques con programas secuestradores. Existe el riesgo potencial de que esas pólizas obstaculicen inadvertidamente las investigaciones delictivas y la notificación de incidentes relacionados con programas secuestradores. Las pólizas de este tipo podrían facilitar la concesión rápida de las exigencias de rescate, con lo cual se podría eludir la obligación de involucrar inmediatamente a las fuerzas del orden y perpetuar así el ciclo de actividades delictivas con programas secuestradores. Esta situación pone de relieve las incertidumbres y complejidades asociadas a los incidentes relacionados con programas secuestradores, y sus posibles implicaciones en materia de aplicación de la ley y ciberseguridad.

Para que la cobertura de un seguro contra riesgos cibernéticos sea útil en caso de que se produzca un ataque con programas secuestradores, debe incluir los siguientes elementos:

- Protección frente a programas secuestradores. Las pólizas de seguros pueden cubrir los costos asociados a un ataque con programas secuestradores, como los pagos de rescate, los honorarios de asesoramiento jurídico y los gastos de recuperación de datos.
- Servicios de respuesta a incidentes. Muchas pólizas de seguros cubren el acceso a servicios de respuesta a incidentes, que pueden proporcionar apoyo y orientación en forma inmediata en caso de que se produzca un ataque con programas secuestradores.
- Evaluación de riesgos de ciberseguridad. Es posible que los proveedores de seguros ofrezcan servicios de evaluación de riesgos para ayudar a las organizaciones a detectar vulnerabilidades en sus estrategias de ciberseguridad y proporcionar orientación sobre cómo mitigar esos riesgos.
- Interrupción de las operaciones. Es posible que las pólizas de seguros cubran la interrupción de la actividad mercantil para proteger a las organizaciones de la pérdida de ingresos y otros gastos derivados de un ataque con programas secuestradores.
- Relaciones públicas. Es posible que las aseguradoras ofrezcan cobertura en materia de relaciones públicas para ayudar a las organizaciones a gestionar su reputación tras sufrir un ataque con programas secuestradores.
- Responsabilidad por filtraciones de datos. Es posible que las pólizas de seguros incluyan cobertura de responsabilidad por filtraciones de datos para proteger a las organizaciones frente a las reclamaciones derivadas de la revelación de datos personales o sensibles.

- Ciberextorsión. Es posible que las aseguradoras ofrezcan cobertura por intentos de extorsión, incluidos aquellos que impliquen la amenaza de un ataque con programas secuestradores.
- Fraude de ingeniería social. Es posible que las pólizas de seguros cubran las pérdidas resultantes del fraude de ingeniería social, como las estafas de suplantación de identidad u otros tipos de ataques de ingeniería social, que, como es sabido, se encuentran entre los principales vectores de infección con programas secuestradores.
- Investigaciones forenses. Es posible que las pólizas de seguros cubran las investigaciones forenses, que pueden ayudar a las organizaciones a determinar la causa y el alcance de un ataque con programas secuestradores.
- Recuperación de datos. Es posible que las pólizas de seguros incluyan cobertura de recuperación de datos, que proporcione apoyo financiero para afrontar el costo de recuperar los datos perdidos o dañados tras un ataque con programas secuestradores.

Cabe señalar que, en el momento de elaborar el presente documento, los seguros contra riesgos cibernéticos no estaban disponibles de forma generalizada en todos los Estados Miembros.

Gestión de incidentes

Cuando se produce un ataque con programas secuestradores, la organización debería aplicar varios planes y políticas para responder de manera eficaz al incidente y minimizar sus repercusiones, empezando por la política de respuesta a incidentes y siguiendo por los planes de continuidad de las operaciones y recuperación en casos de desastre. El primer paso después de descubrir el incidente es evaluar las repercusiones y los riesgos que conlleva. En función del perfil de la organización, es posible que haya que constituir un equipo de tareas integrado por interesados internos y, en su caso, también externos que apoye el proceso de adopción de decisiones. El equipo de tareas debería aprovechar los conocimientos y la experiencia de todos sus miembros para determinar el alcance de la infección, establecer medidas de contención y proponer planes de erradicación. Se deben recopilar las pruebas digitales pertinentes desde el inicio del incidente con el fin de facilitar la evaluación y la investigación que se realizará internamente o será llevada a cabo por los organismos encargados de hacer cumplir la ley. Se debería contactar con los asociados internacionales a través de los cauces existentes o de los organismos intergubernamentales para reunir los conocimientos y las experiencias más recientes en relación con una cepa específica de programa secuestrador. También es conveniente averiguar si existen herramientas de descifrado para el tipo de programa secuestrador concreto[14].

Grado de preparación para la investigación

Contar con capacidades internas para investigar incidentes con programas secuestradores y otros ciberataques puede ser fundamental para localizar rápidamente el origen y el alcance de un ataque con programas secuestradores. Además, puede proporcionar información de inteligencia valiosa que se puede aprovechar durante las negociaciones del rescate, en caso de que se considere necesaria esa línea de acción. Aunque puede que no todas las empresas y organizaciones quieran

[14] Véanse, por ejemplo, No More Ransom (www.nomoreransom.org) y los sitios web de otras empresas de ciberseguridad.

o puedan dotarse de amplias capacidades internas de investigación, esto es un activo vital en el caso de las empresas que se encargan del funcionamiento de infraestructuras críticas y procesan volúmenes considerables de datos sensibles.

Las organizaciones deberían considerar la posibilidad de establecer puntos de contacto en los organismos encargados de hacer cumplir la ley y los EREI o equipos de respuesta a incidentes de seguridad informática de ámbito local. Esos puntos de contacto pueden proporcionar una valiosa ayuda para identificar y rastrear a los autores de los ataques con programas secuestradores. También pueden aportar información esencial sobre las últimas variantes y tendencias en el ámbito de los programas secuestradores.

Rastreo de transacciones y recuperación de rescates pagados

Para poder rastrear las transacciones relacionadas con programas secuestradores hasta llegar a los perpetradores y recuperar los rescates pagados se requiere una amplia gama de capacidades técnicas, jurídicas y financieras. Se trata de tareas complejas y difíciles que precisan un elevado nivel de conocimientos especializados, colaboración interinstitucional a nivel nacional e internacional y acceso a tecnología avanzada.

La amenaza que suponen los programas secuestradores, por su amplia presencia y su capacidad para superar fronteras, debería animar a los Estados Miembros a crear y mantener capacidades para investigar delitos financieros facilitados por los activos virtuales, con arreglo a las normas internacionales de lucha contra el blanqueo de dinero y la financiación del terrorismo, desde la detección de transacciones ilícitas hasta la incautación y el decomiso de activos virtuales. Muchos países todavía no han aplicado las normas internacionales de lucha contra el blanqueo de dinero y la financiación del terrorismo relativas a activos virtuales y PSAV. El GAFI está elaborando medidas para apoyar a los países con capacidades menos desarrolladas que deseen avanzar en la aplicación de esas normas y ha publicado orientaciones actualizadas para adoptar un enfoque basado en los riesgos en relación con los activos virtuales y los PSAV[15], en las que se describe a grandes rasgos cómo se les aplican las normas de lucha contra el blanqueo de dinero y la financiación del terrorismo.

Capacidades para rastrear y recuperar activos virtuales

Los Estados Miembros podrían considerar la posibilidad de desarrollar algunas de las políticas y capacidades más críticas para poder rastrear y recuperar activos virtuales, entre las que se incluyen las siguientes:

- Elaborar un marco legislativo integral que incluya las siguientes disposiciones:
  - la obligación de notificar a los organismos encargados de hacer cumplir la ley o los reguladores financieros los incidentes relacionados con programas secuestradores

[15] GAFI, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (París, 2021). Puede consultarse en www.fatf-gafi.org.

y los pagos conexos, en el mínimo plazo posible (preferiblemente en las 24 horas posteriores a que se tenga conocimiento de los hechos y en un máximo de 72 horas)[16];

- la obligación de que los PSAV conserven registros de todas las transacciones relacionadas con pagos de rescate, ya que pueden ayudar a las autoridades a rastrear y recuperar activos virtuales;
- la obligación de aplicar el principio de conocimiento de los clientes y las políticas y procedimientos para combatir el blanqueo de dinero, y de cooperar con las autoridades competentes en la investigación de los pagos de rescate, con arreglo a las orientaciones del GAFI sobre un enfoque basado en los riesgos en relación con los activos virtuales y los PSAV[17];
- sanciones a los PSAV que no cumplan esas obligaciones.

- Desarrollar la capacidad de detectar, localizar y esclarecer las transacciones de activos virtuales e identificar a sus destinatarios, impartiendo formación en el marco del sistema nacional de desarrollo profesional. Eso contribuirá a que los siguientes organismos y agentes competentes dispongan de los conocimientos y aptitudes necesarios y puedan mantenerlos:
  - unidades de inteligencia financiera;
  - organismos encargados de hacer cumplir la ley;
  - fiscales y miembros del poder judicial;
  - reguladores financieros (autoridades de supervisión y vigilancia);
  - autoridades de gestión de activos.
- Elaborar y revisar periódicamente, en coordinación con las organizaciones internacionales pertinentes, los siguientes documentos:
  - procedimientos operativos estándar en materia de detección, decomiso y gestión de activos virtuales;
  - directrices operativas en materia de investigación y enjuiciamiento penal de delitos facilitados por el uso de activos virtuales;
  - modelos para las solicitudes de información a PSAV extranjeros, las solicitudes de asistencia judicial recíproca, los reportes de operaciones sospechosas, las órdenes de incautación y las resoluciones judiciales, entre otros.

[16] Los incidentes relacionados con programas secuestradores o los pagos conexos se deberían notificar a las autoridades competentes lo antes posible, incluyendo la información básica de que se disponga en el momento de la notificación. El proceso de notificación debería incluir también la obligación subsiguiente de proporcionar información más detallada en una fase posterior.

[17] Véase GAFI, *Updated Guidance*.

Conclusión

En poco más de una década desde su lanzamiento, una novedosa clase de activos se ha consolidado con rapidez fuera del sistema financiero tradicional. Este fenómeno se atribuye en gran medida al desarrollo y la adopción generalizada de Internet como medio de comunicación y al avance de la criptografía como disciplina científica. Los resultados de estos adelantos, a los que se hace referencia en el presente documento con el término "activos virtuales", pero que se clasifican con más precisión como "criptoactivos", constituyen un nuevo instrumento financiero que está basado en un registro descentralizado e inmutable de transacciones anónimas (cadenas de bloques) que están protegidas mediante un conjunto de algoritmos criptográficos abiertos. Por su naturaleza, no es posible inutilizar los criptoactivos sin obstaculizar considerablemente o interrumpir por completo el funcionamiento actual de Internet.

Aunque el estatuto jurídico de los criptoactivos sigue siendo objeto de debate, la relación entre los programas secuestradores y los criptoactivos es bidireccional y compleja. Por un lado, el auge de los criptoactivos ha proporcionado a los operadores de programas secuestradores un método de recepción de pagos cómodo, anónimo y difícil de rastrear. Es probable que esto haya contribuido al aumento de ataques con programas secuestradores, ya que reduce el riesgo para los atacantes y les facilita la monetización de sus actividades. Por otro lado, es probable que el incremento de ataques con programas secuestradores haya hecho aumentar a su vez el uso de criptoactivos con fines delictivos. A medida que crece el número de atacantes que recurren a los programas secuestradores como método de generación de ingresos, aumenta la demanda de métodos de pago anónimos y que no se pueden rastrear. Así pues, aunque es discutible si ha sido el auge de los criptoactivos el que probablemente ha facilitado la proliferación de programas secuestradores, o si ha sido la proliferación de estos programas la que ha tenido como consecuencia el aumento del uso de criptoactivos con fines delictivos, la ausencia de autoridades centrales que controlen los criptoactivos, así como la dificultad de atribuir las transacciones, ha causado indudablemente un gran cambio de paradigma que ha tomado por sorpresa a los reguladores financieros y los organismos encargados de hacer cumplir la ley. No obstante, se han logrado ciertos avances en el desarrollo de técnicas y normas para hacer frente a los riesgos relacionados con esos activos.

La decisión de efectuar el pago del rescate para recuperar datos cifrados por un programa secuestrador es compleja y es necesario sopesar y evaluar cuidadosamente sus riesgos (por ejemplo, la posibilidad de explotación adicional por parte de los delincuentes, la falta de garantías de que los datos se vayan a recuperar en su totalidad, las posibles implicaciones jurídicas y éticas y la posibilidad de que el pago fomente nuevas actividades delictivas). Aunque el pago del rescate tal vez se perciba como la solución más práctica en algunas situaciones, nunca debe ser la primera opción que contemplen las víctimas. En todos los casos, debería considerarse obligatorio notificar a las fuerzas del orden. Además, se recomienda, o bien aprovechar los recursos públicos disponibles, o bien intentar recuperar y reconstruir los datos desde cero. También deben tenerse en cuenta las cuestiones de legalidad y cumplimiento asociadas al pago del rescate, por no mencionar la posibilidad de incentivar la delincuencia, sufrir daños a la reputación y daños políticos e invitar a la extorsión reiterada.

Sin embargo, si, tras ponderar y evaluar cuidadosamente los riesgos y los marcos jurídicos aplicables, se considera que el pago del rescate es la única solución factible, se aconseja exigir a los operadores del programa secuestrador que demuestren su capacidad de descifrar los datos antes de comenzar a negociar su recuperación. En todos los casos se debe considerar la posibilidad de recurrir a profesionales con experiencia e informar a las fuerzas del orden sobre el curso de acción seleccionado.

Notificar a las fuerzas del orden dentro de un plazo establecido los incidentes relacionados con programas secuestradores puede hacer que aumenten considerablemente las posibilidades de recuperar el rescate pagado, ya que podría favorecer una mejor cooperación y coordinación con los PSAV, tanto a nivel nacional como internacional. A su vez, esto puede proporcionar a las organizaciones una ventaja estratégica sobre los atacantes y posibilitar el bloqueo y la congelación de los fondos cuando se transfieran a una plataforma centralizada de cambio de criptomonedas.

La recopilación de abundante información sobre el ataque con programas secuestradores y el atacante es crucial para contribuir a la búsqueda de la justicia. La identificación de las personas responsables, junto con la aplicación de sanciones por ese tipo de actividades delictivas, son medidas esenciales para reducir los actuales niveles de impunidad en torno a los ciberataques. La búsqueda de la justicia, sumada a una respuesta organizada que incluya investigaciones financieras de las transacciones de activos virtuales y actividades de recopilación de pruebas digitales, podría repercutir de forma positiva en la probabilidad de recuperar el rescate.

La lucha eficaz contra los programas secuestradores y, en su caso, la recuperación de los rescates pagados requieren la estrecha colaboración de todos los sectores, incluidos los gobiernos, las empresas privadas y la ciudadanía. Se necesitan campañas de sensibilización y educación del público para que se conozca mejor el modo en que los delincuentes que usan programas secuestradores seleccionan y victimizan a las organizaciones, y las maneras en que estas pueden protegerse contra los ataques con programas secuestradores. La cooperación interinstitucional a nivel nacional es fundamental para recuperar con éxito los rescates pagados, ya que permite compartir recursos, como personal especializado e información de inteligencia sobre las actividades de grupos delictivos.

Para que la actuación de la justicia penal y la recuperación de datos en caso de un ataque con programas secuestradores sean satisfactorias, es esencial que exista cooperación internacional en materia de cumplimiento de la ley, ya que ese tipo de ataques pueden originarse en cualquier lugar del mundo y tener como objetivo personas y organizaciones de todo el mundo. Esa cooperación implica compartir información de inteligencia, recursos y conocimientos especializados a fin de determinar y mitigar las repercusiones del ataque. Las alianzas público-privadas también desempeñan un papel fundamental en la recuperación de rescates, ya que combinan las fortalezas de cada sector y permiten a los organismos encargados de hacer cumplir la ley acceder a información e inteligencia valiosas para investigar y enjuiciar a los delincuentes.

La adopción de las normas internacionales de lucha contra el blanqueo de dinero y la financiación del terrorismo relativas a activos virtuales y PSAV es un elemento clave para mitigar los riesgos de blanqueo de dinero relacionados con los programas secuestradores. No obstante, como se mencionó en una actualización reciente del GAFI al respecto[18], en la mayoría de los países evaluados hasta el momento, la aplicación de la recomendación 15 del GAFI sobre nuevas tecnologías todavía no ha alcanzado el estado de "mayoritariamente cumplida". Por consiguiente, es esencial que los gobiernos den prioridad al cumplimiento de esas normas para afrontar de manera eficaz la amenaza de los programas secuestradores y asegurar que los ciberdelincuentes rindan cuentas por sus actos. El marco regulatorio en materia de programas secuestradores debe diseñarse de forma que se pueda adaptar a la naturaleza en constante evolución de los ataques con programas secuestradores y debe tener en cuenta los avances en materia de ciberseguridad y protección de datos. En general, la adopción de las normas recomendadas puede proporcionar un marco amplio para que las organizaciones tomen decisiones fundamentadas en relación con los pagos de rescate y eviten convertirse en una fuente de ingresos para los ciberdelincuentes.

Las organizaciones deben disponer de una estrategia integral para prevenir y gestionar los ataques con programas secuestradores y recuperarse de ellos. Eso conlleva la aplicación de un plan de respuesta a incidentes que incluya políticas de copias de seguridad y recuperación, políticas de ciberseguridad, formación continua del personal e iniciativas de educación y sensibilización. En caso de que se produzca un incidente relacionado con programas secuestradores, la organización debe evaluar las repercusiones y los riesgos, formar un equipo de tareas y utilizar una matriz de evaluación de riesgos y un diagrama de adopción de decisiones para determinar cómo proceder. También es crucial notificar el incidente a las partes interesadas internas y externas pertinentes y mantener canales de comunicación claros, además de documentar todos los procesos y procedimientos para su futura consulta.

La obligación de notificar los incidentes relacionados con programas secuestradores a las fuerzas del orden y las autoridades reguladoras dentro de un plazo establecido y la aplicación de políticas en consonancia con las normas internacionales de lucha contra el blanqueo de dinero y la financiación del terrorismo para rastrear y localizar activos virtuales son elementos cruciales para combatir el uso de programas secuestradores. Ello requiere la elaboración de marcos legislativos amplios, medidas firmes y sostenibles de creación de capacidad y la formulación de directrices operativas armonizadas, en coordinación con las organizaciones internacionales.

[18] GAFI, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (París, 2022). Puede consultarse en www.fatf-gafi.org.

El Programa Mundial contra el Blanqueo de Dinero, la Ocultación del Producto del Delito y la Financiación del Terrorismo y el Programa Mundial contra el Delito Cibernético de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) están decididos a mejorar su asistencia técnica y sus programas de capacitación sobre activos virtuales. Un objetivo clave del Programa Mundial contra el Blanqueo de Dinero, la Ocultación del Producto del Delito y la Financiación del Terrorismo es ayudar a las autoridades competentes de los Estados Miembros a mitigar los riesgos de blanqueo de dinero y financiación del terrorismo asociados al uso de activos virtuales. El programa abarca varios ámbitos, entre los que se incluyen el apoyo legislativo, reglamentario y de supervisión, las evaluaciones nacionales de riesgos, la capacitación personalizada y la orientación en materia de investigación. Su objetivo último es ayudar a los países a cumplir las normas del GAFI y aumentar la eficacia de sus marcos de lucha contra el blanqueo de dinero y la financiación del terrorismo.

UNODC
Oficina de las Naciones Unidas
contra la Droga y el Delito

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

2306141