GAFI

RAPPORT DU GAFI

Lutte contre le financement des rançongiciels

Mars 2023

Le Groupe d'action financière (GAFI) est un organisme intergouvernemental indépendant dont la mission consiste à élaborer et promouvoir des stratégies de protection du système financier mondial face au blanchiment de capitaux, au financement du terrorisme et au financement de la prolifération d'armes de destruction massive. Les Recommandations du GAFI se sont imposées comme les normes internationales en matière de lutte contre le blanchiment de capitaux (LBC) et de financement du terrorisme (LFT).

Pour obtenir des informations complémentaires sur le GAFI, veuillez consulter le site **www.fatf-gafi.org.**

Ce document et/ou toute carte qu'il pourrait contenir est/sont publié(e)s sans préjudice du statut de tout territoire, de la souveraineté s'exerçant sur ce dernier, du tracé des frontières et limites internationales et du nom d'un(e) quelconque territoire, ville ou région quelconque territoire, ville ou région.

Référence de citation :

GAFI (2023), *Lutte contre le financement des rançongiciels,* GAFI, Paris, France, https://www.fatf-gafi.org/fr/publications/methodesettendances/documents/lutte-contre-financement-rancongiciels

Ce document a été traduit par le Ministère des Finances du Canada. La seule version officielle est le texte anglais.

Table des matières

Consulter également :

Lutte contre le financement des rançongiciels : indicateurs de risques

Cette liste d'indicateurs de risque potentiels complète le rapport du Groupe d'action financière sur le blanchiment de capitaux (GAFI), *Counter Ransomware Financing* (lutte contre le financement des rançongiciels), et peut aider les entités des secteurs public et privé à cerner les activités suspectes liées aux rançongiciels.

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

Acronymes

AEP	Autorités d'enquête et de poursuite (AEP)
BC	Blanchiment des capitaux
CC	Cryptomonnaie confidentielle
CERT	Équipes d'intervention en cas d'urgence informatique
CRF	Cellules de renseignements financiers
DS	Déclaration de soupçon
EPNFD	Entreprises et professions non financières désignées
FiDé	Finance décentralisée
GCAV	Groupe de contact des actifs virtuels
HC	Hors cote
IP	Protocole Internet
LBC-LFT	Lutte contre le blanchiment des capitaux et le financement du terrorisme
PPP	Partenariat public-privé
PSAN	Prestataires de service en actifs numériques
RaaS	Ransomware as a service (rançongiciel en tant que service)
RPV	Réseau privé virtuel

Résumé

Au cours des dernières années, les flux financiers liés aux attaques de rançongiciels ont augmenté de manière considérable sur la scène internationale. Les estimations de l'industrie font état de quatre fois plus de paiements de rançongiciels en 2020 et 2021, comparativement à 2019. De nouvelles techniques ont augmenté la rentabilité des attaques et la probabilité de réussite. Ces techniques ciblent de grandes entités de grande valeur ainsi que les rançongiciels en tant que service, où les criminels de rançongiciels vendent des gammes de logiciels faciles à utiliser aux affiliés. Les conséquences des attaques de rançongiciels peuvent être désastreuses et constituer des menaces pour la sécurité nationale, notamment en endommageant et en perturbant les infrastructures et les services cruciaux.

Grâce à cette étude, le GAFI cherche à améliorer la compréhension internationale des flux financiers liés aux rançongiciels et à souligner les bonnes pratiques pour faire face à cette menace. Le rapport fournit également une liste d'indicateurs de risque qui aideront les autorités et le secteur privé à détecter ces flux financiers. Les conclusions de ce rapport s'appuient sur l'expérience et l'expertise des secteurs public et privé, notamment les contributions et les études de cas de plus de 40 délégations du réseau mondial du GAFI.

Une attaque de rançongiciel est une forme d'extorsion. Les normes du GAFI exigent qu'elle soit criminalisée en tant qu'infraction sous-jacente au blanchiment des capitaux. Ce rapport révèle que les paiements et le blanchiment ultérieur des produits des rançongiciels sont presque exclusivement effectués au moyen d'actifs virtuels. Les criminels utilisant des rançongiciels exploitent la nature internationale des actifs virtuels pour faciliter des transactions transfrontalières quasi instantanées à grande échelle, parfois sans l'implication des institutions financières traditionnelles qui ont des programmes de lutte contre le blanchiment des capitaux et le financement du terrorisme (LBC-FT). Les criminels compliquent davantage leurs transactions en utilisant des technologies, des techniques et des jetons confidentiels dans le processus de blanchiment, tels que les cryptomonnaies et les mélangeurs confidentiels.

L'utilisation quasi exclusive d'actifs virtuels dans le blanchiment lié aux rançongiciels renforce davantage l'importance d'accélérer la mise en œuvre de la recommandation 15 du GAFI, obligeant les États à mettre en place des mesures pour atténuer les risques liés aux actifs virtuels et réglementer les prestataires de services d'actifs virtuels (PSAV). Ces efforts sont essentiels pour empêcher les criminels d'accéder facilement aux PSAV relevant d'États où les contrôles de LBC-FT sont faibles ou inexistants pour blanchir le profit de leurs crimes.

Ce rapport constate également que les attaques de rançongiciels sont généralement sous-signalées, que ce soit en raison de difficultés de détection par le secteur privé, de répercussions négatives sur l'entreprise de la victime ou de la crainte de représailles de la part des criminels lorsqu'une victime signale une attaque. Cela explique en partie le manque d'expérience dans les enquêtes sur le blanchiment des capitaux lié aux rançongiciels. Les États doivent poursuivre leurs efforts pour augmenter et améliorer les sources de détection et de signalement. Les autorités doivent agir rapidement pour recueillir les renseignements clés et devraient disposer des outils et des compétences nécessaires pour localiser et récupérer efficacement les actifs virtuels.

Les rançongiciels couvrent un large éventail de domaines, et les enquêtes peuvent impliquer des acteurs externes aux autorités traditionnelles de LBC-FT, comme les organismes de cybersécurité et de protection des données. Une approche multidisciplinaire est donc nécessaire pour lutter efficacement contre les rançongiciels et le blanchiment des capitaux connexe. En raison de la nature intrinsèquement décentralisée et transfrontalière des actifs virtuels, il est impératif de renforcer et d'exploiter les mécanismes de coopération internationale actuels pour lutter efficacement contre le blanchiment lié aux rançongiciels.

Pour renforcer la réponse mondiale contre les rançongiciels et le blanchiment connexe, le GAFI propose aux États de prendre les mesures énumérées au paragraphe suivant.

Mesures proposées

Les renseignements recueillis dans le cadre de cette étude ont fourni quelques exemples pratiques de mesures que les pays peuvent prendre pour améliorer leur capacité à lutter contre les flux financiers illicites liés aux rançongiciels. Cette section résume ces pratiques exemplaires et formule des suggestions sur la manière dont les États pourraient empêcher plus efficacement le blanchiment des capitaux lié aux rançongiciels.

Mettre en œuvre les normes pertinentes du GAFI, notamment les normes relatives aux PSAV, et améliorer la détection :

- Les États devraient accélérer la mise en conformité avec les normes pertinentes du GAFI relatives aux PSAV en mettant en œuvre la recommandation 15 (y compris la règle d'acheminement [1]) dès que possible. Cette recommandation garantit le respect des obligations LBC-FT nécessaires aux PSAV pour obtenir des renseignements financiers critiques et signaler les opérations suspectes.
- Les États devraient veiller à ce que les rançongiciels soient criminalisés en tant qu'infraction principale de blanchiment de capitaux, conformément à la recommandation 3 du GAFI (en tant que type d'extorsion, par exemple).
- Les gouvernements devraient améliorer la détection des rançongiciels en :
  - prêtant main-forte aux entités réglementées à détecter les rançongiciels et le blanchiment de capitaux connexe et à signaler les opérations suspectes, notamment en communiquant les tendances, les guides de détection et les indicateurs d'alerte (comme ceux contenus dans *Lutter contre*

[1] La « règle d'acheminement » est une mesure clé en matière de LBC-FT, obligeant les PSAV à obtenir, conserver et échanger des renseignements sur les donneurs d'ordre et les bénéficiaires de virements d'actifs virtuels. Cela permet aux institutions financières et aux PSAV d'effectuer un contrôle des sanctions et de détecter les opérations suspectes.

le financement des rançongiciels : indicateurs de risque potentiels[2]) aux entités déclarantes concernées.

- encourageant les victimes à signaler volontairement les incidents, par exemple en les sensibilisant au soutien et aux ressources disponibles ou en créant des canaux sûrs de signalement.

- De plus, les États devraient envisager d'établir des canaux de communication avec des acteurs non traditionnels qui peuvent ne pas être soumis aux exigences de LBC-FT (comme les entreprises de cyberassurance et de réponse aux incidents), afin d'augmenter les sources de détection.

Promouvoir les enquêtes financières et les efforts de recouvrement des actifs

- Les autorités compétentes devraient utiliser et adapter, au besoin, les techniques d'application de la loi traditionnelles, ainsi que les techniques propres aux actifs virtuels, pour mener des enquêtes sur le blanchiment de capitaux liés aux rançongiciels. Les autorités compétentes devraient disposer des compétences spécialisées et de l'expertise nécessaires pour mener à bien les enquêtes financières relatives aux rançongiciels. Cela comprend la création d'analyses de chaînes de blocs et d'outils de surveillance, l'accès à ceux-ci, ainsi que la formation à cet égard.

- Les États devraient veiller à ce que les autorités de poursuite pénale disposent des capacités et des pouvoirs nécessaires pour saisir et confisquer rapidement et efficacement les actifs, en particulier les avoirs virtuels, et à ce que les autorités conservent ces capacités et pouvoirs. Les États devraient s'assurer que des mécanismes spécialisés sont en place pour gérer les actifs virtuels saisis de manière convenable.

Adopter une approche multidisciplinaire pour lutter contre les rançongiciels

- Les gouvernements devraient veiller à cibler et à évaluer les risques de blanchiment des capitaux posés par les rançongiciels dans leurs évaluations nationales des risques. Compte tenu de la nature décentralisée des actifs virtuels et des groupes criminels de rançongiciels, cela comprend les États possédant des secteurs d'actifs virtuels pour lesquels les rançongiciels ne constituent pas, pour l'instant, une menace nationale. De telles constatations peuvent, en outre, contribuer à soutenir les cyberstratégies nationales en obtenant une vue d'ensemble nationale globale des risques liés aux rançongiciels.

[2]Consulter le rapport : https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/countering-ransomware-financing.html

- Les États devraient élaborer des mécanismes de coordination entre les autorités compétentes concernées, allant des autorités de poursuite pénale, de la LBC-FT et de la cybercriminalité, aux partenaires non traditionnels tels que les organismes de cybersécurité ou de protection des données. Cela favorise l'échange de renseignements et fournit une plateforme utile pour l'échange croisé de diverses expertises techniques.

Soutenir les partenariats avec le secteur privé

- Les États devraient cibler et établir des mécanismes soutenant la coopération entre le secteur public et le secteur privé. Les États devraient envisager l'implication des PSAV et d'autres partenaires non traditionnels dans ces mécanismes de coopération. Cela permettra de créer des plateformes utiles pour sensibiliser, échanger des expertises et des idées, ainsi que soutenir les objectifs en matière d'application de la loi.

Améliorer la coopération internationale

- Les pays devraient établir des mécanismes bilatéraux, régionaux et multilatéraux, et y participer activement en utilisant, par exemple, des bureaux de liaison et en établissant des points de contact clairs et disponibles en tout temps, afin de faciliter une coopération internationale et un échange de renseignements rapides. Ainsi, il est possible de soutenir efficacement la détection rapide des fonds transfrontaliers et le recouvrement efficace des actifs. Ces mécanismes aident également les autorités à démanteler les réseaux transnationaux impliqués dans les rançongiciels et le blanchiment de capitaux connexe.

Introduction

Sujet et portée

1. Un rançongiciel est un type de logiciel malveillant (malware) que les criminels développent ou utilisent pour refuser l'accès aux données, aux systèmes ou aux réseaux tout en exigeant le paiement d'une rançon pour débloquer ces accès. Parmi les attaques courantes, on retrouve le cryptage des données, la fuite de données et l'interruption des opérations des victimes. Bien souvent, ces attaques impliquent plusieurs méthodes et peuvent être accompagnées d'une menace de publication des données de la victime[3].

2. Les incidents liés aux rançongiciels ont considérablement augmenté ces dernières années[4], tant en nombre qu'en ampleur. Les rançongiciels cherchent, avant tout, à tirer des profits, et la croissance des attaques a entraîné une augmentation conséquente des produits des rançongiciels et du blanchiment de capitaux connexe. Les estimations de l'industrie indiquent que les paiements de rançongiciels ont au moins quadruplé en 2020 et 2021, comparativement à 2019[5]. Bien que les dernières données de l'industrie suggèrent une tendance à la baisse en 2022 (probablement parce que les victimes refusaient de payer), la valeur des actifs virtuels reçus par les personnes derrière les rançongiciels reste nettement plus élevée qu'avant 2019[6]. Le nombre total réel d'attaques et de pertes liées à ces attaques est susceptible d'être considérablement plus élevé, car les attaques de rançongiciels sont souvent passées sous silence.

3. Les attaques ont provoqué des interruptions et des dommages majeurs au sein des gouvernements, des institutions publiques, des entreprises et auprès des citoyens. Dans certains cas, les systèmes de santé ont même été touchés, menaçant ainsi la sécurité nationale et entraînant l'interruption d'infrastructures et de services critiques ou des brèches de sécurité en matière de données de nature délicate[7]. Les criminels tirant les ficelles des rançongiciels ont élaboré des techniques pour augmenter la rentabilité de leurs attaques et leurs chances de réussite. Par conséquent, la menace de flux financiers illicites liés aux rançongiciels continuera probablement de croître.

---

[3] FBI « Scams and Safety : Ransomware » (consulté en septembre 2022), en anglais seulement : www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware; Australian Cyber Security Center « Ransomware » (consulté en septembre 2022), en anglais seulement : www.cyber.gov.au/ransomware.

[4] ENISA Threat Landscape 2022 (octobre 2022), en anglais seulement : www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[5] Chainalysis, « Chainalysis Crypto Crime Report 2022 » (février 2022), en anglais seulement : https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

[6] Chainalysis, « Ransomware Revenue Down As More Victims Refuse to Pay » (janvier 2023), en anglais seulement : https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/

[7] Les attaques contre les hôpitaux, par exemple, ont compromis les soins aux patients, et les attaques envers les services de police ont eu une incidence sur la sécurité.

4. Les criminels exigent presque uniquement des paiements de rançongiciels en actifs virtuels. Les victimes, ou des tiers connexes agissant au nom d'une victime, utilisent souvent des prestataires de services d'actifs virtuels (PSAV)[8] pour payer des rançons. Les criminels derrière les attaques de rançongiciels utilisent également les PSAV pour blanchir des fonds illicites et échanger les produits contre de la monnaie fiduciaire, qui peut être échangée plus facilement contre des biens et des services et constitue une réserve de valeur plus stable.

5. En 2018, le GAFI a modifié ses recommandations pour couvrir les actifs virtuels et les PSAV. Le GAFI a depuis publié diverses directives pour aider les pays et le secteur privé à surveiller et à atténuer les risques dans ce secteur, notamment les indicateurs d'alerte du blanchiment de capitaux (BC) et du financement du terrorisme (FT)[9]. Bien que ces travaux aient souvent abordé les rançongiciels, ce rapport est la première instance où le GAFI se concentre expressément sur les tendances et les techniques de blanchiment liées aux attaques de rançongiciels.

6. Le GAFI tire parti de l'expérience du gouvernement singapourien en matière d'enquêtes financières impliquant des actifs virtuels pour cibler les défis et échanger des pratiques exemplaires de lutte contre le financement des rançongiciels et le blanchiment de capitaux connexe. Le présent rapport se concentre sur la manière de cibler et de signaler les paiements liés aux rançongiciels, la manière de prévenir, détecter et enquêter sur les flux financiers provenant de rançongiciels, ainsi que sur la manière dont ces produits sont blanchis. Le présent rapport ne se concentre pas sur l'utilisation de rançongiciels pour le financement du terrorisme en raison de l'absence d'utilisation significative ou notable de rançongiciels à cette fin, selon les renseignements et les études de cas soumises dans le cadre de ce rapport.

7. Puisqu'une attaque de rançongiciel est une forme d'extorsion, les recommandations du GAFI exigent que tous les États criminalisent le blanchiment de capitaux lié aux rançongiciels (R.3). Le GAFI exige également que les États ciblent, évaluent et prennent des mesures pour atténuer leurs risques de blanchiment de capitaux (R.1-2). Les États doivent veiller à ce que le secteur privé, notamment les PSAV, applique des mesures préventives suffisantes, comme le signalement des opérations suspectes (R.9-23). Les États doivent veiller à ce que les autorités de poursuite pénales enquêtent, localisent et confisquent les produits du crime (R.4, 29-31). Les États doivent coopérer au niveau international pour lutter contre le blanchiment de capitaux, les infractions sous-jacentes, ainsi que les produits subséquents (R.36-40).

---

[8] Le terme « prestataire de services d'actifs virtuels » désigne toute personne physique ou morale qui n'est pas couverte ailleurs par les recommandations et qui, en tant qu'entreprise, exerce une ou plusieurs des activités ou opérations suivantes pour ou au nom d'une autre personne physique ou morale : échange d'actifs virtuels contre des monnaies fiduciaires; échange entre une ou plusieurs formes d'actifs virtuels; transfert d'actifs virtuels; conservation et administration d'actifs virtuels ou d'instruments permettant le contrôle d'actifs virtuels; participation aux services financiers liés à l'offre d'un émetteur ou à la vente d'actifs virtuels et prestation de tels services.

[9] Consulter les rapports du GAFI suivants, en anglais seulement : *Targeted Update on Implementation of the FATF Standards on Virtual Assets And Virtual Asset Service Providers* (juin 2022); *Virtual Assets Red Flag Indicators* (septembre 2020); et *Confidential FATF Guidance on Financial Investigations Involving Virtual Assets (août 2019).*

8. Bien que les rançongiciels soient un type de cybercrimes, les renseignements contenus dans le présent rapport se concentrent sur les rançongiciels et peuvent, ou non, s'appliquer à d'autres types de cybercrimes, tels que les logiciels malveillants, l'hameçonnage de courriels professionnels ou la compromission et la vente de renseignements financiers.

Objectifs et structure

9. La partie I du présent rapport illustre la manière dont les criminels utilisant des rançongiciels reçoivent, blanchissent et encaissent leurs produits illicites. Elle vise à sensibiliser le monde entier et à mieux comprendre l'ampleur de la menace internationale que sont les rançongiciels, la manière dont les paiements de rançongiciels ou les paiements connexes sont effectués, ainsi que la manière dont les produits découlant d'attaques de rançongiciels sont mis à la disposition des cybercriminels.

10. La partie II cible les défis et les pratiques exemplaires pour discerner les flux financiers liés aux rançongiciels et enquêter sur ceux-ci, afin de les interrompre.

11. Le présent rapport vise à aider les **autorités opérationnelles** à produire des renseignements financiers de haute qualité, à mener des enquêtes financières et à cerner, localiser et saisir les produits illicites. **Les autorités de réglementation nationale** et les **décideurs politiques** peuvent utiliser les renseignements fournis dans le présent rapport pour cerner les vulnérabilités et atténuer les risques. Cela aidera également les **institutions financières**, les **PSAV** et les **entreprises et professions non financières désignées (EPNFD)** à concevoir et à mettre en œuvre des contrôles pour détecter, signaler et prévenir les mouvements illicites de produits liés aux rançongiciels.

Méthodologie

12. Des experts d'Israël et des États-Unis ont dirigé conjointement ce projet. De plus, les États et entités suivantes ont contribué aux travaux dans le cadre de l'équipe du projet : l'Australie, le Canada, la Commission européenne, la France, l'Allemagne, le Japon, le Luxembourg, le Mexique, les Philippines, Singapour, l'Afrique du Sud, l'Espagne, la Suisse, la Turquie, le Royaume-Uni, le groupe Asie-Pacifique sur le blanchiment des capitaux et le Groupe Egmont des cellules de renseignement financier.

13. Les conclusions du présent rapport sont fondées sur les éléments suivants :

- Une revue des documents existants et non classifiés à ce sujet.
- Une demande au réseau mondial du GAFI, qui regroupe plus de 200 pays, pour obtenir des renseignements sur les points de vue des États au sujet des risques, sur les lois et pouvoirs nationaux, sur les défis et les pratiques exemplaires, ainsi que sur des études de cas liées aux rançongiciels. L'équipe de projet a reçu la contribution de plus de 40 délégations.

- Des discussions au sein du groupe de contact des actifs virtuels (GCAV) du GAFI[10].
- Un engagement ciblé avec le secteur privé, par l'intermédiaire du GCAV.

[10]En juin 2019, le groupe d'élaboration des politiques a convenu de créer le groupe de contact sur les actifs virtuels pour transmettre les exigences du GAFI au secteur privé, et pour veiller à ce que l'industrie élabore rapidement des solutions technologiques appropriées pour mettre en œuvre ces exigences.

PARTIE I. FLUX FINANCIERS PROVENANT DES RANÇONGICIELS

Ampleur des flux financiers

14. L'ampleur des attaques de rançongiciels et des flux financiers connexes a considérablement augmenté dans le monde entier. Au cours des dernières années, de nombreux États ont remarqué une augmentation de la fréquence des attaques de rançongiciels, allant d'une croissance de 10 % à plusieurs centaines de pour cent, selon le pays. De ce fait, le nombre de signalements par les victimes s'est proportionnellement accru, et le nombre de déclarations de soupçons liés aux rançongiciels a également augmenté parmi les divers pays. Dans le cas d'un État, les déclarations de soupçons déposées au cours des six premiers mois de 2021 ont relevé l'équivalent de 590 millions de dollars américains (552 millions euros) en opérations liées aux rançongiciels, soit une augmentation de 42 % par rapport à 2020, où le total atteignait les 416 millions de dollars américains (389 millions euros)[11]. De récents rapports annuels d'organismes chargés de l'application de la loi montrent une croissance importante des activités de rançongiciels[12], et les estimations de l'industrie montrent une croissance semblable du nombre d'attaques et de types actifs de rançongiciels. En 2021, le nombre estimé d'attaques de rançongiciels était d'environ 623,3 millions, soit plus du double des 304,6 millions d'attaques estimées en 2020[13]. De même, le nombre estimé de types actifs de rançongiciels aurait doublé par rapport à 2019[14].

15. Bien que certains pays ont signalé de faibles niveaux d'attaques de rançongiciels, les renseignements recueillis dans le cadre du présent rapport montrent que les attaques de rançongiciels sont toujours sous-déclarées, même si le nombre de déclarations de soupçons et de signalements par les victimes a augmenté dans certains États. Il est donc difficile d'estimer le nombre total exact d'incidents et les sommes payées en rançons. Les études de cas soumises pour le présent rapport ont montré que les rançongiciels peuvent constituer un risque pour les pays développés et en voie de développement, peu importe la région.

16. Plusieurs pays ont déterminé que l'augmentation des attaques de rançongiciels et des flux financiers connexes était liée à l'élaboration de techniques par des criminels utilisant des rançongiciels, comme **Big game hunting (chasse au gros gibier)**, **les rançongiciels en tant que service (RaaS)**, **les tactiques d'extorsion double, triple ou multiple**, afin de maximiser l'efficacité et la rentabilité des attaques (consulter l'encadré 1).

---

11 FINCEN, « Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021 » (juin 2021), en anglais seulement : www.fincen.gov/sites/default/files/2021-10/Financial Trend Analyse Ransomware 508 FINAL.pdf

12 FBI, « Internet Crime Report 2021 » (consulté le 1er décembre 2022), en anglais seulement : www.ic3.gov/Home/AnnualReports
EUROPOL, « Internet Organized Crime Threat Assessment (IOCTA) 2021 » (consulté le 1er décembre 2022), en anglais seulement : www.europol.europa.eu/publications-events/main-reports/iocta-report

13 SonicWall, « 2022 SonicWall Cyber Threat Report » (2022), en anglais seulement : www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf

14 Chainalysis, « Chainalysis Crypto Crime Report 2022 » (février 2022), en anglais seulement : https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

Encadré 1. Élaboration de techniques de rançongiciels

Les criminels utilisant des rançongiciels utilisent la **chasse au gros gibier** pour cibler d'importantes organisations de grande valeur ou des entités de premier plan qui, selon eux, sont plus susceptibles de payer une rançon pour reprendre leurs activités commerciales ou éviter un examen du public. Les criminels utilisant des rançongiciels ciblent également, de manière sélective, les organisations exploitant des chaînes d'approvisionnement avec une production juste-à-temps, car elles sont plus susceptibles d'avoir des coûts de temps d'arrêt plus élevés, ainsi que des infrastructures essentielles et des organisations détenant des renseignements précieux ou de nature délicate. Les attaquants peuvent juger que ces organisations ont une propension plus élevée à payer des rançons par rapport aux autres victimes.

RaaS désigne un modèle commercial criminel grâce auquel les criminels utilisant des rançongiciels fournissent des gammes de logiciels de rançons sur le Web clandestin ou sous-traitent des éléments d'attaques de rançongiciels, notamment la distribution de logiciels malveillants, la compromission initiale du réseau d'une victime, la fuite de données, ou la négociation d'une rançon pour les affiliés en échange d'une commission ou d'un pourcentage de la rançon. Les criminels peuvent aussi acheter des renseignements d'identification volés pour accéder aux systèmes des victimes et en tirer profit, ce qui permet la diffusion de rançongiciels. Les criminels peuvent ainsi obtenir des renseignements sur des industries précises dans un pays précis pour orienter la sélection de leur victime et maximiser l'efficacité de leur attaque. Le modèle RaaS a réduit les coûts et l'expertise technique nécessaires pour mener des attaques de rançongiciels, diminuant les obstacles et permettant aux criminels moins expérimentés de mener des attaques de rançongiciels.

La double extorsion désigne une pratique où les exploitants de rançongiciels obtiennent les données d'une victime avant de les chiffrer, puis menacent de publier les données volées si les demandes de rançons ne sont pas payées. Cette menace de divulgation s'ajoute à la menace liée à l'interruption des systèmes. Cette tactique peut exercer une pression supplémentaire sur les victimes afin qu'elles paient des demandes de rançon, et ce même si elles peuvent rétablir les activités.

La triple extorsion désigne une pratique où les exploitants de rançongiciels demandent de l'argent non seulement à la victime qui a été ciblée en premier, mais également à une victime qui pourrait être touchée par la divulgation des données de la première victime, comme des renseignements médicaux protégés, des renseignements permettant d'identifier une personne, des identifiants de compte ou une propriété intellectuelle.

L'extorsion multiple désigne une pratique impliquant plus de deux méthodes d'extorsion. Cette pratique se base sur une double extorsion utilisant le cryptage et la divulgation de données, mais comprend des tactiques de pression supplémentaires, comme une attaque par déni de service distribuée (DDoS), la communication avec les clients des victimes, la vente à découvert des actions des victimes ou encore l'interruption des systèmes d'infrastructure.

17. Selon les informations publiques, plus de la moitié des attaques de rançongiciels signalées a ciblé des membres du gouvernement ou de la fonction publique et le secteur des biens et services industriels[15,16]. Cette situation est probablement causée, en partie, par la chasse au gros gibier, qui peut représenter des paiements importants et une augmentation globale des paiements de rançongiciels. Les criminels utilisant des rançongiciels ont également ciblé les institutions de l'énergie, financières, de communication et d'éducation au cours des dernières années. Bien que les criminels utilisant des tactiques de chasse au gros gibier peuvent se concentrer sur des victimes plus imposantes, les petites et moyennes entreprises ou industries sont également fortement ciblées par les attaques de rançongiciels. En fait, les attaques de rançongiciels ciblent principalement toujours les petites et moyennes entreprises. Ces cibles plus petites peuvent avoir un rapport risque-bénéfice plus cohérent par rapport aux attaques plus médiatisées contre des victimes plus importantes. Au deuxième trimestre de 2020, près de 55 % des attaques ont eu lieu contre des entreprises de moins de 100 employés, et environ 75 % des attaques ont eu lieu contre des entreprises dont le chiffre d'affaires est inférieur à 50 millions de dollars américains (47 millions d'euros)[17].

18. Les montants des rançons vont de quelques centaines de dollars ou d'euros d'actifs virtuels dans le cas de petites attaques visant des particuliers, à des millions de dollars ou d'euros pour les cas ciblant de grandes entreprises, plus précisément des infrastructures critiques ou des organisations détenant des renseignements précieux ou de nature délicate. Les expériences des pays indiquent que la somme de la rançon demandée par les criminels a également augmenté au cours des dernières années. Le paiement moyen d'une rançon était d'environ l'équivalent de 800 000 dollars américains (748 000 euros) en actifs virtuels pour 2021, soit près de cinq fois plus qu'en 2020[15]. Cette augmentation est probablement liée à l'utilisation des techniques de chasse au gros gibier que nous avons susmentionnées. Dans certains cas, les demandes de rançon ont atteint des dizaines de millions de dollars ou d'euros en actifs virtuels. En voici

[15] Sophos, « The State of Ransomware in State and Local Government » (septembre 2022), en anglais seulement : https://assets.sophos.com/X24WTUEQ/at/rbjqpp5wwm6v5h3wj9v3733/sophos-state-of-ransomware-government-2022-wp.pdf.

[16] Digital Shadows, « Ransomware: Analyzing The Data From 2020 » (janvier 2021), en anglais seulement : www.digitalshadows.com/blog-and-research/ransomware-analyzing-the-data-from-2020/.

[17] Coveware, « Q2 Quarterly Report » (août 2020), en anglais seulement : www.coveware.com/blog/q2-2020-ransomware-marketplace-report.

un exemple : selon des articles de presse de 2021, une compagnie d'assurance basée aux États-Unis a été attaquée par un « Phoenix CryptoLocker » (qui serait le troisième plus grand RaaS en termes de revenus en 2021 après Conti et Darkside) [18] et aurait payé 40 millions de dollars américains (37 millions d'euros) pour reprendre le contrôle de son réseau[19].

Caractéristiques et tendances géographiques

19. Généralement, les rançongiciels sont un phénomène international, en partie en raison de la nature de la cybercriminalité et des actifs virtuels. Les renseignements du réseau mondial du GAFI, les études de cas et les données de l'industrie relèvent certaines caractéristiques et tendances géographiques des attaques de rançongiciels. De nombreux réseaux de rançongiciels ont été liés à des États présentant des risques de blanchiment de capitaux plus élevés (consulter l'encadré 2). Dans de nombreux cas, les criminels utilisant des rançongiciels déposent ou encaissent leurs produits dans ces pays. Dans d'autres cas, des attaques de rançongiciels ont été menées à partir de ces pays, et il est possible que les pays concernés aient parrainé ces attaques[20].

[18] Chainalysis, « Chainalysis Crypto Crime Report 2022 » (février 2022), en anglais seulement : https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

[19] Mehrotra, Kartikay et Turton, William, « CNA Financial Paid $40 Million in Ransom After March Cyberattack », Bloomberg, 20 mai 2021 (consulté le 1er décembre 2022), en anglais seulement : www.bloomberg.com/news /articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-mars-cyberattack

[20] Consulter l'alerte (AA22-187A) de la U.S. Cybersecurity et Infrastructure Security Agency (juillet 2022), en anglais seulement : www.cisa.gov/uscert/ncas/alerts/aa22-187a.

Encadré 2. États présentant des risques de blanchiment d'argent plus élevés

Bien qu'il n'existe pas de définition ou de méthodologie universelle pour déterminer si un État présente un risque plus élevé de blanchiment de capitaux ou de financement du terrorisme, le fait de tenir compte des risques propres au pays, en conjonction avec d'autres facteurs de risque, fournit des renseignements utiles pour cibler davantage ces risques. Les indicateurs de risque plus élevé comprennent : a) les pays ou les zones géographiques désignés par des sources fiables comme fournissant un financement ou un soutien aux activités terroristes ou qui ont des organismes désignés comme terroristes opérant en leur sein; b) les pays désignés par des sources fiables comme présentant des niveaux importants de crime organisé, de corruption ou d'autres activités criminelles, y compris les pays d'origine ou de transit pour les drogues illicites, la traite de personnes, la contrebande et les jeux de hasard illégaux; c) les pays qui font l'objet de sanctions, d'embargos ou de mesures similaires imposées par des organismes internationaux, comme les Nations Unies; d) les pays désignés par des sources fiables comme ayant des régimes de gouvernance, d'application de la loi et de réglementation faibles, y compris les pays ciblés par les déclarations du GAFI comme ayant des régimes de LBC-FT faibles, plus précisément en ce qui a trait aux PSAV, et pour lesquels les PSAV et autres entités assujetties devraient accorder une attention particulière aux relations d'affaires et aux opérations.

Source : GAFI (2021), « Updated Guidance for a Risk-Based Approach: Virtual Assets and VASPs », paragraphe 154.

20. L'ampleur des attaques de rançongiciels diffère d'une région à l'autre. Selon les rapports de l'industrie de 2022, la région du Moyen-Orient et de l'Afrique était la moins ciblée par les attaques de rançongiciels (4 %), suivie de l'Amérique latine (6 %), de l'Asie-Pacifique (10 %), de l'Europe (28 %) et de l'Amérique du Nord. (52 %)[21]. L'écart d'ampleur entre les régions géographiques a eu une incidence sur la façon dont ces régions perçoivent le risque que présentent les rançongiciels. Les renseignements fournis par le réseau mondial du GAFI montrent que les pays connaissant une augmentation de la chasse au gros gibier et des rançons majeures connexes sont plus susceptibles d'évaluer les risques de blanchiment des capitaux liés aux rançongiciels comme étant élevés.

21. De nombreux grands groupes de rançongiciels exploitent une version de RaaS appelée modèle d'affiliation, à l'aide de laquelle ils sous-traitent des éléments de l'attaque de rançongiciels en échange d'une commission ou d'un pourcentage de la rançon. Dans de tels cas, ces criminels sont souvent dispersés aux quatre coins du monde, compliquant ainsi l'identification et la localisation des parties

[21] Group-IB, « Ransomware Uncovered Report. Group-IB » (mai 2022), en anglais seulement : https://spiresolutions.com/wp-content/uploads/2021/07/ransomware_uncovered_2020.pdf.

impliquées dans les attaques de rançongiciels. Par exemple, comme l'illustre l'étude de cas d'Emotet ci-dessous, les criminels utilisant des rançongiciels peuvent coopérer pour mener des attaques ou utiliser une infrastructure commune tout en opérant à partir de différents pays. La variété des criminels impliqués dans divers pays peut également compliquer la surveillance des flux monétaires liés aux principaux criminels rançongiciels.

Encadré 3. Étude de cas sur Emotet[1]

Emotet est l'une des campagnes de logiciel malveillant les plus importantes de ces dernières années. Il a été découvert pour la première fois en tant que cheval de Troie bancaire[2] en 2014, devenant un outil clé pour d'autres logiciels malveillants et rançongiciels. Au moment du démantèlement du réseau, en janvier 2021, Emotet impliquait jusqu'à 70 % des logiciels malveillants du monde entier, notamment RYUK et DoppelPaymer, qui ont eu une grave incidence économique sur les entreprises britanniques. Le démantèlement a impliqué une collaboration étroite entre les AEP du Canada, de la France, de l'Allemagne, de la Lituanie, des Pays-Bas, de l'Ukraine, du Royaume-Uni et des États-Unis, ainsi qu'une activité internationale coordonnée par Europol et Eurojust. Grâce à ce partenariat collaboratif, les AEP nationaux ont été en mesure de cibler et analyser les données reliant les détails de paiement et d'enregistrement aux criminels qui utilisaient Emotet. L'affaire illustre l'ampleur et la nature de la cybercriminalité, prouvant à quel point la coopération internationale est essentielle pour lutter contre la menace.

Source : Royaume-Uni

Notes :

1. Consulter également le communiqué de presse d'Europol sur Emotet, en anglais seulement : www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-perturbé par une action globale
2. Un cheval de Troie bancaire désigne un logiciel malveillant qui tente de voler les authentifiants des clients d'une institution financière ou d'accéder à leurs renseignements financiers.

22. Le blanchiment des paiements de rançongiciels est également transnational compte tenu de la nature transfrontalière des actifs virtuels, avec lesquels les paiements de rançongiciels sont presque toujours effectués. Les utilisateurs d'actifs virtuels peuvent effectuer des transactions entre pairs en effectuant des transactions directement entre eux, en utilisant uniquement leur clé privée et une connexion Internet, indépendamment des frontières géographiques et sans la participation d'institutions ayant des obligations en matière de LBC-FT. Les criminels, notamment les criminels utilisant des logiciels de rançon et ayant accès à Internet, peuvent exploiter les caractéristiques des actifs virtuels pour faciliter les opérations transfrontalières quasi instantanées à grande échelle, et ce sans intermédiaires financiers traditionnels dotés de programmes de LBC-FT. Ils ont également accès à des PSAV basés dans le monde entier, dans des États où les contrôles de LBC-FT sont faibles ou inexistants, que les criminels exploitant

des rançongiciels utilisent pour encaisser leurs produits illicites en monnaie fiduciaire.

Encadré 4. Qu'est-ce qu'un actif virtuel?

Un actif virtuel est une représentation numérique de la valeur qui peut être échangée ou transférée numériquement. Il peut être utilisé à des fins de paiement ou d'investissement. Les actifs virtuels ne comprennent pas les représentations numériques des monnaies fiduciaires, des valeurs mobilières et d'autres actifs financiers qui sont déjà abordés ailleurs par les recommandations du GAFI.

Les actifs virtuels les plus couramment utilisés sont un moyen d'échange où les enregistrements de génération ou de propriété sont pris en charge grâce à une technologie de registre distribué (DLT) qui repose sur la cryptographie. Les chaînes de blocs, par exemple, sont issues d'une DLT. Comme l'indique le paragraphe suivant, de nombreux actifs virtuels populaires fonctionnent sur des chaînes de blocs publiques, où des renseignements de transaction sous le couvert de pseudonymes sont visibles.

Source : GAFI

Méthodes et tendances courantes

23. Afin de mener une enquête financière efficace sur une attaque de rançongiciel, il faut une solide compréhension des méthodes et des techniques utilisées pour blanchir des fonds. Puisque les attaques de rançongiciels sont généralement sous-déclarées, le présent rapport a rassemblé des renseignements provenant de diverses sources ouvertes ainsi que les expériences de certains pays, afin de mieux comprendre la manière dont les paiements de rançon sont effectués, blanchis, reçus et, dans certains cas, échangés contre de la monnaie fiduciaire.

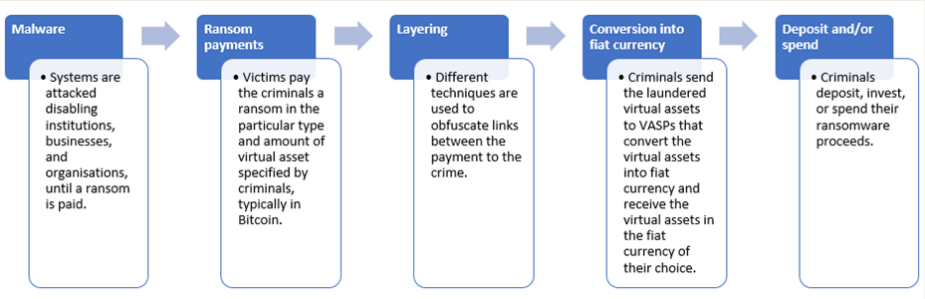
24. Les flux financiers liés aux rançongiciels impliquent bien souvent plusieurs institutions financières traditionnelles et des PSAV. D'autres tiers, tels que les compagnies de cyberassurance, les entreprises d'intervention en cas d'incident ou les entreprises de cybersécurité, peuvent également être impliqués dans la réponse à une attaque de rançongiciel, y compris dans le cadre du processus de paiement de la victime.

25. Bien que les actifs virtuels soient la méthode de paiement des rançongiciels principale, les flux financiers globaux liés aux rançongiciels impliquent plusieurs institutions financières traditionnelles, des PSAV et des tiers supplémentaires.

Tableau 1. Types de secteurs d'activités pouvant être impliqués dans les flux financiers des rançongiciels

Institutions financières	Les institutions financières agissent généralement en tant qu'intermédiaires qu'utilisent les victimes de rançongiciels (ou un tiers agissant au nom de la victime) pour transmettre des fonds à un PSAV afin d'acheter des actifs virtuels.
PSAV	Les victimes de rançongiciels (ou un tiers agissant au nom de la victime) ont recours aux PSAV pour acheter et transférer le type précis et la quantité d'actifs virtuels exigés par le criminel derrière le rançongiciel.
Compagnies d'assurance	Les compagnies d'assurance peuvent couvrir et parfois payer une rançon dans le cadre d'une couverture de cyberassurance.
Entreprises d'intervention en cas d'incident	Les entreprises d'intervention en cas d'incident engagées par les victimes de rançongiciels négocient souvent le paiement de la rançon avec les attaquants. Ces entreprises peuvent acheter les actifs virtuels des PSAV dans le cadre de leurs services, pour le paiement de la rançon, et les transférer aux criminels au nom des victimes.
Entreprises de cybersécurité	Ces entreprises sont chargées de protéger les données, les systèmes, les réseaux et les appareils connectés du client contre tout accès non autorisé et illégal.

Encadré 5. Flux financiers typiques liés aux paiements de rançongiciels :



Une victime ayant reçu une demande de rançon, ou tout autre tiers agissant en son nom, enverra habituellement les fonds à un PSAV par virement électronique, par chambre de compensation automatisée ou par carte de crédit, afin d'acheter le type et la quantité d'actifs virtuels demandés par le criminel derrière le rançongiciel. Les tiers qui agissent pour le compte de la victime peuvent être des sociétés d'intervention en cas d'incident ou des compagnies d'assurance cybernétique.

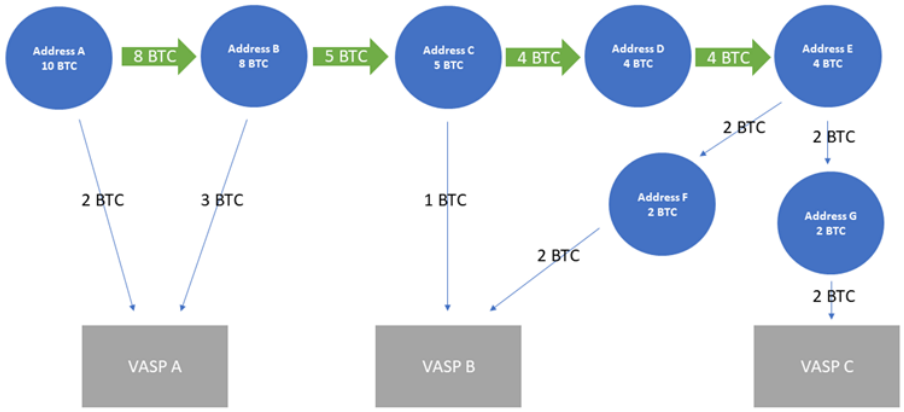
Ensuite, la victime ou le tiers enverra le paiement de la rançon, bien souvent à partir d'un portefeuille hébergé chez un PSAV, à l'adresse de l'actif virtuel de l'auteur du crime. Il s'agit généralement d'un portefeuille non hébergé (un logiciel ou un ordinateur permettant aux utilisateurs de détenir, de stocker et de transférer des actifs virtuels sans l'implication d'un tiers, tel qu'un PSAV [communément appelé portefeuille sans dépositaire]) contrôlé par un criminel utilisant un rançongiciel ou une mule financière. Il peut également s'agir d'un portefeuille hébergé par un PSAV résident à l'extérieur du pays d'origine de l'attaque et qui ne coopère généralement pas avec les autorités chargées de la LCB-FT ou les CRF.Dans bien des cas, le criminel utilisant un rançongiciel recourra à diverses techniques visant à simplifier la dispersion (ces techniques seront détaillées un peu plus loin). Enfin, les criminels derrière un rançongiciel utilisent souvent des PSAV situés dans des pays autres que les pays où ils se situent pour échanger des actifs virtuels contre de la monnaie fiduciaire, bien qu'ils puissent également laisser des fonds dans des portefeuilles non hébergés pendant de longues périodes ou utiliser des actifs virtuels pour payer des tiers impliqués dans les attaques.

26. Les criminels derrière les rançongiciels utilisent souvent des technologies, des techniques et des jetons confidentiels dans le processus de blanchiment, notamment un ou plusieurs des éléments ci-dessous. Les criminels ne peuvent pas utiliser les mêmes éléments à chaque fois ni suivre le même ordre lors du blanchiment de leurs profits.

- Les attaquants de rançongiciels exigent souvent que les paiements des victimes sous forme d'actifs virtuels soient envoyés aux adresses de portefeuilles qu'ils contrôlent, et souvent à **différentes adresses de portefeuille** pour recevoir les revenus illicites de chaque attaque.

- Une fois que les attaquants ont reçu des fonds, ils peuvent utiliser plusieurs adresses intermédiaires pour déplacer les actifs virtuels d'une adresse de portefeuille vers de nouvelles adresses en rafales, à l'aide d'une série d'opérations transférant de petites sommes d'actifs virtuels. Les fonds sont généralement envoyés à des adresses de portefeuille hébergées par plus d'un PSAV. Ces modèles d'opérations, communément appelés **chaînes de pelage (*peel chains*)**, ne sont pas seulement utilisés pour masquer le mouvement des actifs virtuels[22]. Ils peuvent également être exploités par des criminels pour blanchir une grande quantité d'actifs virtuels au moyen d'une série d'opérations mineures dans le but de réduire les possibilités de remonter à la source de ce comportement. La piste des actifs virtuels peut être masquée, par exemple, si les opérations sont exécutées rapidement et fréquemment.

Figure 1. Illustration de chaînes de pelage



- De plus, les criminels utilisant des rançongiciels blanchissent souvent des actifs virtuels au moyen de **mélangeurs** (comme Wasabi) qui utilisent diverses méthodes pour dissimuler le lien entre l'adresse qui envoie les actifs virtuels et les adresses qui les reçoivent. Les mélangeurs sont utilisés soit comme une solution de rechange, soit en plus du mouvement des actifs virtuels dans la chaîne de pelage. Dans certains cas, les cybercriminels utilisent les opérations CoinJoin, dans lesquelles plusieurs expéditeurs et destinataires de fonds combinent leurs paiements en une seule opération globale. Il faut alors, dans la plupart des cas, un service spécialisé tel que JoinMarket qui regroupe les utilisateurs intéressés et leur permet de réaliser une telle opération.

[22] Des chaînes de pelage sont observées sur une base régulière et peuvent se produire naturellement en raison de la conception des portefeuilles d'actifs virtuels.

- De plus, bien que la plupart des criminels demandent un paiement Bitcoin, il arrive également que ces derniers aient recours à des **cryptomonnaies confidentielles**. Les expériences des États et les rapports de l'industrie indiquent que les cryptomonnaies confidentielles sont utilisées pour payer les attaquants, car elles peuvent brouiller les portefeuilles expéditeurs et destinataires. Par exemple, elles peuvent utiliser une combinaison de technologies renforçant la confidentialité, telles que les mélangeurs, la signature de cercle (*ring signature*), les adresses furtives et les algorithmes en signature de cercle, qui peuvent brouiller les adresses de portefeuilles expéditeurs et destinataires. Un nombre croissant de criminels utilisant des rançongiciels demandent des paiements exclusivement en Monero, bien que l'actif virtuel le plus couramment utilisé dans les cas de rançongiciels soit le Bitcoin (99 % des cas)[23]. Certains pays ont constaté des cas où des attaquants ont accepté des paiements à la fois en Bitcoin et en Monero. Cependant, ils factureraient des frais supplémentaires allant de 10 à 20 % de la rançon demandée pour les paiements Bitcoin, car ces opérations peuvent être localisées plus facilement. Ainsi, les criminels paieront des frais supplémentaires pour utiliser des technologies renforçant l'anonymat, comme les mélangeurs, afin de compliquer la tâche des autorités souhaitant localiser ou identifier les auteurs des opérations.
- Plusieurs pays ont également remarqué que les cybercriminels convertissent souvent le paiement de la rançon de Bitcoin en d'autres actifs virtuels grâce à des PSAV ou des protocoles de FiDé[24,25]. Cette mesure est souvent appelée **saut de chaîne (*chain-hopping*)** et désigne le déplacement d'un actif virtuel vers une autre chaîne de blocs, généralement en succession rapide, afin d'échapper aux tentatives de suivi de ces mouvements. Un État a signalé que les criminels utilisant des rançongiciels ont de plus en plus recours à des protocoles de FiDé pour accéder à des cryptomonnaies dites stables[26] avant de convertir des fonds en monnaie fiduciaire. Les plateformes de FiDé sont attrayantes pour les criminels, car beaucoup d'entre elles ne mettent pas en œuvre de contrôles de LBC-FT, même si elles peuvent être soumises à ces obligations en fonction des faits et circonstances de leurs modèles commerciaux. Un État a notamment

23 Coveware, « Q3 Ransomware Marketplace Report » (novembre 2019), en anglais seulement : www.coveware.com/blog/q3-ransomware-marketplace-report.

24 Le terme « finance décentralisée » (FiDé) est utilisé lorsque des applications décentralisées ou distribuées, activées par le contrat intelligent (*smart-contract*) d'une chaîne de blocs avec supervision centrale (*provisioned blockchain*), offrent des services financiers, tels que ceux proposés par les PSAV. Une application de FiDé (c'est-à-dire un logiciel) n'est pas un PSAV aux termes des normes du GAFI, car les normes ne s'appliquent pas aux logiciels ou à la technologie sous-jacents. Cependant, les créateurs, propriétaires et exploitants, ou certaines autres personnes qui conservent un contrôle ou une influence suffisante dans les ententes de FiDé, peuvent correspondre à la définition d'un PSAV établie par le GAFI lorsqu'ils fournissent ou facilitent activement des services de PSAV.

25 En plus d'être utilisés pour blanchir les paiements de rançongiciels, les protocoles de FiDé eux-mêmes, en particulier les ponts interchaînes, sont de plus en plus ciblés par les cybercriminels qui cherchent à exploiter les failles de sécurité et à voler des actifs virtuels.

26 Remarque sur la terminologie : Le GAFI considère que le terme « cryptomonnaie stable » n'est pas une catégorie juridique ou technique claire, mais plutôt un terme que les promoteurs de cryptomonnaie emploient lors de leurs campagnes de promotion. Afin d'éviter de soutenir involontairement leurs affirmations, le présent rapport emploiera donc le terme « cryptomonnaie dite stable ».

signalé avoir remarqué que les criminels derrière les rançongiciels utilisent régulièrement des protocoles de FiDé et des mélangeurs, parfois même en plusieurs suites lors du processus de blanchiment des capitaux.

- Au cours du processus de blanchiment, les criminels utilisant des rançongiciels impliquent des PSAV centralisés, notamment des négociateurs hors cote, pour encaisser leurs profits. Les criminels envoient les actifs virtuels à un PSAV situé dans un pays à haut risque ou à un PSAV avec des contrôles de LBC-FT faibles ou inexistants aux fins de conversion en monnaie fiduciaire. Pour ce faire, les criminels se situant dans des États à haut risque peuvent être en mesure d'utiliser des PSAV centralisés locaux, comme dans le cas de ceux désignés par les États-Unis (Suex[27], Chatex[28], Garantex[29] et Bitzlato [consulter l'encadré 6 ci-dessous])[30]. Plusieurs pays ont signalé que les installations d'encaissement étaient fortement concentrées dans les centres urbains. Dans certains cas, les criminels derrière les rançongiciels de divers groupes ont utilisé les mêmes PSAV pour recevoir ou blanchir leurs actifs virtuels.
- Dans les cas où plusieurs tiers sont impliqués, les criminels utilisant des rançongiciels doivent habituellement payer des partenaires criminels et des hébergements d'infrastructure. Les exploitants d'infrastructures criminelles sont de plus en plus disposés à accepter un paiement en actifs virtuels, et les criminels utilisant des rançongiciels effectuent fréquemment ces paiements en utilisant le produit de leurs attaques. Dans de nombreux cas, les entreprises d'analyse de chaînes de blocs ont observé des détournements directs de paiements de rançongiciels vers des adresses d'actifs virtuels associés à des exploitants criminels malveillants « d'infrastructures en tant que service ».

27 Consulter le communiqué de presse du Trésor américain, en anglais seulement : https://home.treasury.gov/news/press-releases/jy0364

28 Consulter le communiqué de presse du Trésor américain, en anglais seulement : https://home.treasury.gov/news/press-releases/jy0364

29 Consulter le communiqué de presse du Trésor américain, en anglais seulement : https://home.treasury.gov/news/press-releases/jy0701

30 Consulter le communiqué de presse du ministère américain de la Justice, en anglais seulement : www.justice.gov/opa/pr/founder-and-majority-owner-cryptocurrency-exchange-charged-processing-over-700-million

Encadré 6. Bitzlato [1]

Une opération transnationale a permis de constater, en janvier 2023, que Bitzlato, un bureau de change virtuel ayant des activités importantes en Russie, jouait un rôle essentiel dans le blanchiment de monnaie virtuelle convertible (MVC). Les autorités françaises et américaines ont mené cette opération avec le soutien d'Europol et la participation des autorités belges, chypriotes, portugaises, espagnoles et néerlandaises. Bitzlato était soupçonné d'avoir ouvert la voie à diverses opérations illicites, notamment pour des criminels utilisant des rançongiciels tels que Conti, un groupe de RaaS affilié à la Russie. Le ministère américain de la Justice a également allégué que Bitzlato avait reçu plus de 15 millions de dollars en produits de rançongiciels. En parallèle, la CRF américaine (Financial Enforcement Network) a rendu une ordonnance désignant la plateforme comme une « préoccupation majeure en matière de blanchiment des capitaux ».

Ces enquêtes ont permis le démantèlement de la plateforme d'échange, notamment la saisie d'infrastructures numériques et d'actifs criminels de 18 millions d'euros dans des portefeuilles de cryptomonnaie en France, ainsi que l'arrestation d'individus clés dans divers pays.

Bitzlato s'est fait connaître comme étant une plateforme exigeant une identification minimale de la part de ses utilisateurs et, en raison de ces procédures déficientes de connaissance du client,, Bitzlato serait devenu un refuge pour les produits du crime et les fonds destinés à des activités criminelles.

Source : France et États-Unis

1. Consulter également le communiqué de presse de la Gendarmerie nationale française à l'adresse suivante : www.gendarmerie.interieur.gouv.fr/gendinfo/enquetes/2023/demantelement-d-une-plateforme-de-cryptomonnaies-servant-au- blanchissement
Consulter également le communiqué de presse d'Europol, en anglais seulement : www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested

27. Certains pays ont également remarqué que les criminels utilisant des rançongiciels employaient des **mules financières** ayant des comptes chez des PSAV pour reconvertir les produits en monnaie fiduciaire grâce à des rampes de sortie. Ces rampes sont des services ou des plateformes permettant l'échange d'actifs virtuels contre de la monnaie fiduciaire (une pratique communément appelée « encaissement »). De tels comptes peuvent être créés à l'aide d'une identité volée ou fausse ou peuvent être détenus de manière légitime par un tiers complice de l'utilisation du compte. En général, les mules financières sont des tiers non associés impliqués dans la dernière étape du processus de blanchiment des capitaux et qui sont responsables d'une partie des fonds transitant par un réseau de blanchiment. Leur dissociation de l'entité criminelle et leurs transferts de moindre valeur peuvent les rendre plus difficiles à identifier.

Encadré 7. Exemple de recrutement de mules financières

Les criminels utilisant des rançongiciels recrutent des mules financières et leur fournissent des appareils mobiles. Dans la plupart des cas, ces mules financières n'ont aucune présence sur Internet et sont peu informées à ce sujet. Des courriels sont ensuite créés chez des fournisseurs de services de courriel anonymes en dehors du pays. Il devient alors difficile d'identifier les utilisateurs de ces courriels. Les mules financières utilisent un appareil mobile fourni par le « gestionnaire » criminel pour les processus d'intégration et pour créer un compte auprès de l'institution financière ou du PSAV. Une fois l'intégration terminée, les mules financières rendent l'appareil au « gestionnaire » criminel. Les « gestionnaires » criminels utilisent ces appareils au nom de la mule financière pour effectuer des opérations en ligne. Les criminels profitent parfois des services de réseau privé virtuel (RPV) qui rendent l'adresse IP (protocole Internet) de l'appareil utilisé anonyme. Par conséquent, l'emplacement géographique réel du criminel effectuant des opérations reste masqué.

Source : Afrique du Sud

PARTIE II. DÉFIS ET PRATIQUES EXEMPLAIRES EN MATIÈRE D'INTERRUPTION DU BLANCHIMENT DE CAPITAUX DÉCOULANT DE RANÇONGICIELS

Cadre juridique

28. Un cadre juridique solide sert de point de départ pour permettre aux autorités compétentes d'élaborer des politiques efficaces d'atténuation des risques liés aux rançongiciels. Cette section analyse la pertinence des normes du GAFI pour (i) la criminalisation des rançongiciels en matière de blanchiment des capitaux et (ii) l'imposition de mesures préventives aux secteurs réglementés concernés.

Rançongiciel en tant qu'infraction sous-jacente du blanchiment des capitaux

29. Bien que la plupart des pays n'aient pas de législation pénale spécifique aux rançongiciels, cela ne les empêche généralement pas de poursuivre en justice pénale les attaques de rançongiciels en tant qu'infraction sous-jacente[31].

30. Selon les contributions des participants au projet, les États ont tendance à poursuivre l'infraction sous-jacente de rançongiciel soit par des accusations d'extorsion, soit, plus communément, à titre de crime informatique, comme des dommages aux données, une intrusion ou des dommages aux programmes et systèmes informatiques. La recommandation 3 du GAFI exige que les États criminalisent le blanchiment de capitaux lié aux infractions d'extorsion. Les infractions d'extorsion ont habituellement l'avantage d'être neutres sur le plan technologique, ce qui signifie qu'elles peuvent comprendre les attaques de rançongiciel, quelle que soit la méthode ou la forme. Les pays ayant recours aux infractions d'extorsion devraient veiller à ce que leurs lois demeurent pertinentes pour permettre aux autorités compétentes d'enquêter et de récupérer efficacement les flux illicites d'actifs virtuels (consulter la section 6).

31. Contrairement à l'extorsion, les crimes informatiques ne font pas partie de la liste minimale des infractions sous-jacentes du GAFI[32]. Cela ne semble toutefois pas entraîner des lacunes dans la poursuite du blanchiment de capitaux découlant de l'activité des rançongiciels dans la pratique. Selon un échantillon de pays, ceux qui utilisent les crimes informatiques pour poursuivre les rançongiciels en justice considèrent ces infractions comme étant sous-jacentes (soit dans la liste désignée des infractions sous-jacentes, soit à l'aide d'une « approche tous crimes »). Dans le cadre de cette étude, aucun pays n'a signalé de problème pour intenter des poursuites judiciaires contre le blanchiment de capitaux lié aux rançongiciels. Néanmoins, les pays devraient veiller à ce que leur choix d'accusation d'infraction sous-jacente n'entrave pas leur capacité à engager des poursuites contre le blanchiment de capitaux lié aux rançongiciels.

---

31 La plupart des pays ont également indiqué qu'ils n'incriminaient pas les victimes payant des rançons aux auteurs d'attaques de rançongiciels, bien que certains d'entre eux découragent fortement les victimes de payer les rançons.

32 Consulter les catégories désignées d'infractions définies dans le glossaire des recommandations du GAFI.

Imposition de mesures préventives aux acteurs concernés

32. Les normes du GAFI exigent que les États adoptent des mesures pour prévenir le blanchiment de capitaux, notamment par l'intermédiaire des institutions financières, des EPNFD et des PSAV. Ces mesures garantissent que ces entités comprennent et atténuent leurs risques de blanchiment de capitaux en appliquant les contrôles appropriés, notamment l'identification de leurs clients, et en détectant et en signalant les opérations suspectes, conformément aux recommandations 9 à 23 du GAFI.

33. Compte tenu de la relation entre les rançongiciels et les actifs virtuels, la modification apportée aux normes du GAFI en 2018, pour appliquer ces mesures aux PSAV, a été une étape importante dans l'amélioration du régime mondial de LBC-FT contre les risques posés par les rançongiciels. Mais en janvier 2023[33], sur les 86 pays évalués à l'aide des normes révisées (recommandation 15), seuls 63 (73 %) se conformaient partiellement ou ne se conformaient pas du tout à ces exigences[34]. Parmi l'ensemble des pays évalués, seulement l'un d'entre eux était pleinement conforme.

34. Compte tenu de l'éventail de pays évalués à l'aide de la recommandation 15 révisée, il est probable que ces chiffres soient fortement représentatifs de la situation dans l'ensemble du réseau mondial du GAFI. Cette évaluation est en outre étayée par les conclusions d'une enquête menée par le GAFI en mars 2022 et qui a révélé qu'en 2022, moins de la moitié des répondants disposaient d'un régime de licence ou d'enregistrement pour les actifs virtuels et les PSAV. Il existe donc fort probablement des lacunes dans l'application des obligations de LBC-FT par les PSAV, notamment en matière d'identification des clients ou de signalement des opérations suspectes, dans la plupart des pays. Il est important que les pays membres du réseau mondial accélèrent la mise en conformité avec la recommandation 15 (y compris la règle d'acheminement), en raison de la nature transfrontalière des actifs virtuels.

---

[33] Consulter les notations d'évaluation consolidées à l'adresse suivante : www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-ratings.html. Il convient toutefois de noter que ce ne sont pas tous les pays qui ont été évalués à l'aide de la méthodologie révisée de la recommandation 15.

[34] Cette analyse est fondée sur l'évaluation mutuelle et les rapports de suivi des États qui ont été évalués selon la méthodologie révisée de la recommandation 15.

Mesures proposées

- Les États devraient accélérer la mise en conformité avec les normes pertinentes du GAFI relatives aux PSAV en mettant en œuvre la recommandation 15 (y compris la règle d'acheminement) dès que possible. Cette recommandation garantit le respect des obligations LBC-FT nécessaires aux PSAV pour obtenir des renseignements financiers critiques et signaler les opérations suspectes.
- Les États devraient veiller à ce que les rançongiciels soient criminalisés en tant qu'infraction principale de blanchiment de capitaux, conformément à la recommandation 3 du GAFI (en tant que type d'extorsion, par exemple).

Détection et signalement

35. En raison de la répartition géographique des criminels utilisant des rançongiciels, de leur utilisation des techniques de blanchiment de capitaux et des caractéristiques actuelles des attaques de rançongiciels (comme indiqué dans la partie I ci-dessus), il est difficile d'estimer l'ampleur des flux financiers dérivés de ce phénomène. Les attaques de rançongiciels demeurent sous-signalées dans la plupart des pays. Il devient alors difficile de brosser un portrait complet des gains et des flux financiers découlant des rançongiciels.

36. La réussite des enquêtes financières s'appuie sur une détection et un signalement solides des attaques (consulter l'encadré 6 ci-dessous). Selon l'expérience des pays et des études de cas soumises, il existe deux sources principales pour détecter les flux financiers liés aux rançongiciels : les déclarations de soupçons et les signalements par les victimes. Cette section explore les défis et bonnes pratiques en ce qui concerne le champ d'application des exigences en matière de déclarations de soupçons, d'identification des transactions suspectes, d'encouragement à la déclaration des victimes et autres sources de détection.

Portée des obligations de déclaration de soupçons

37. Les autorités compétentes utilisent couramment les déclarations de soupçons pour détecter les attaques de rançongiciels et à titre de source de renseignements lors des enquêtes. À ce jour, la majeure partie des déclarations de soupçons relatives aux paiements de rançongiciels sont déposées par les PSAV et les banques.

38. Quelques pays ont identifié des secteurs qui ne sont généralement pas soumis aux obligations de LBC-FT en tant que sources potentielles supplémentaires de détection des produits illicites liés aux rançongiciels. Il pourrait être utile d'encourager les secteurs non traditionnels à signaler les opérations suspectes, ou encore d'imposer le signalement à ces secteurs, en particulier lorsqu'ils sont directement impliqués dans la résolution des attaques de rançongiciels au nom de leurs clients.

39. Par exemple, le secteur de l'assurance au sens large, notamment les institutions impliquées dans les rançongiciels et la cyberassurance, peut posséder des renseignements directs sur les attaques de rançongiciels impliquant des clients cyberassurés déposant des demandes de remboursement. Ces entités ne sont pas visées par la définition du GAFI d'« institution financière », qui couvre la souscription et le placement d'assurance-vie et d'autres assurances liées aux investissements. Cependant, en s'engageant avec le secteur pour encourager ou exiger la déclaration, certaines juridictions ont constaté un premier impact positif sur la déclaration des rançongiciels.

Commented [MMF1]: For consistency, continue using.

Encadré 8. Sensibilisation ciblée auprès du secteur de l'assurance pour améliorer le signalement de rançongiciels

En France, le secteur de l'assurance non-vie est soumis aux exigences de LBC-FT. Une campagne de sensibilisation a été menée auprès de ce secteur en 2021 par l'intermédiaire de groupes de travail spécialisés réunissant des représentants de l'ensemble des secteurs public et privé. Ces groupes de travail avaient pour objectif d'étudier l'assurabilité des risques numériques et de renforcer la résilience des entreprises face aux cyberattaques. Un rapport publié[1] par ces groupes de travail couvrant, entre autres, l'évolution des risques de blanchiment de capitaux liés aux rançongiciels, ainsi que les obligations de LBC-FT et les pratiques exemplaires relatives au paiement et au remboursement des rançons, s'est avéré constituer un document essentiel.

L'Autorité de contrôle prudentiel et de résolution (ACPR) a en outre exercé un contrôle prudentiel précis sur les compagnies d'assurance, y compris lors de contrôles sur place. L'ACPR a ensuite rappelé aux entités réglementées leurs exigences en matière de LBC-FT lorsqu'elles font appel à de tels services, notamment la nécessité de surveiller et d'obtenir toute information financière pertinente (surtout pour la surveillance des paiements).

Depuis, TRACFIN a constaté une augmentation des déclarations de soupçons liées aux paiements de rançongiciels déposées par le secteur de l'assurance, passant de 19 en 2019 et 28 en 2020, à 66 en 2021. L'augmentation de 2021 est en partie due à une seule compagnie d'assurance, et les volumes ne sont pas encore suffisamment importants pour en tirer des conclusions ou des résultats.

Source : France

1. En français seulement : www.banque-france.fr/sites/default/files/rapport_45_f.pdf

40. Les entreprises d'intervention en cas d'incident ont également accès à des renseignements pertinents relatifs aux attaques et aux paiements de rançongiciels. Ces entreprises, telles que les entreprises d'enquête numérique et de réponse aux incidents et les cabinets d'avocats, aident les victimes à répondre aux attaques de rançongiciels. Elles peuvent faciliter les paiements de rançongiciels versés aux cybercriminels en négociant les sommes demandées par les rançongiciels, en convertissant la monnaie fiduciaire des clients en actifs virtuels et en transférant les fonds vers des comptes contrôlés par des criminels. Le fait d'encourager ou d'exiger les signalements par ce secteur permet de détecter et de signaler les attaques de rançongiciels en temps opportun, d'autant plus que les clients sont susceptibles d'informer ces entités dès le départ (dans certains cas, avant d'en informer les AEP). En fonction du modèle économique et des services qu'elles fournissent, ces entreprises peuvent également correspondre à la définition d'un PSAV (et par conséquent, être soumises aux obligations de déclarations de soupçons et de LBC-FT) si elles agissent en tant qu'entreprise pour une autre personne physique ou morale ou au nom de celle-

ci, si elles échangent des actifs virtuels contre d'autres actifs virtuels ou une monnaie fiduciaire, ou bien si elles transfèrent, conservent ou administrent des actifs virtuels.

Encadré 9. Réglementation des entreprises d'enquête numérique et de réponse aux incidents (EINRI)

Les entreprises d'EINRI et les compagnies de cyberassurance peuvent aider les victimes d'attaques de rançongiciels en fournissant des services qui simplifieront les paiements de rançongiciels. En 2020 et 2021, le FinCEN (la CRF des États-Unis) a précisé dans des avis sur les rançongiciels[1] que, selon les faits et les circonstances, cette activité pourrait constituer un transfert d'argent. Les entités impliquées dans les transferts de fonds sont tenues de s'enregistrer en tant qu'entreprise de transfert de fonds et sont assujetties aux obligations de LBC-FT. Les avis comprenaient également des indicateurs d'alerte financière ou des rançongiciels et leurs paiements connexes pour les entreprises d'EINRI et les compagnies de cyberassurance, afin de soutenir la détection d'activités suspectes et le dépôt de rapports d'activités suspectes (RAS).

Au cours des six premiers mois de 2021, les rapports soumis par des entreprises d'EINRI basées aux États-Unis ont représenté environ 63 % des RAS liés aux rançongiciels[2]. Dans l'ensemble, le FinCEN a constaté une augmentation de 188 % du nombre de rapports reçus en 2021. Ces rapports ont permis au FinCEN d'analyser et de découvrir des tendances et des renseignements sur celles-ci, afin de soutenir les efforts pangouvernementaux de prévention et de lutte contre les attaques de rançongiciels. Par exemple, l'analyse du FinCEN a révélé que tout au long de 2021, les rançongiciels ont représenté une menace importante continue pour les secteurs des infrastructures critiques, les entreprises et le public américains. De plus, l'analyse a souligné que les variants de rançongiciels liés à la Russie étaient responsables de la majorité des activités de rançongiciels signalées, représentant 69 % de la valeur des incidents de rançongiciels et 75 % des incidents liés aux rançongiciels au cours des six derniers mois de 2021[3].

Source : États-Unis

Notes
1. En français seulement : www.banque-france.fr/sites/default/files/rapport_45_f.pdf
2. Consulter l'analyse des tendances financières du FinCEN, en anglais seulement : www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf
3. Consulter l'analyse des tendances financières du FinCEN, en anglais seulement : www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf

41. L'encadré précédent illustre l'utilité d'encourager ou d'exiger les signalements auprès d'un large éventail d'entités déclarantes non traditionnelles en fonction du risque et du contexte. Cela permet de signaler et de cerner les activités suspectes dans différents secteurs, améliorant ainsi la capacité des autorités à découvrir et à détecter des incidents autrement inconnus en rassemblant des renseignements sur différents secteurs.

Mesures visant à améliorer la détection d'opérations suspectes

42. Les pays reconnaissent que les activités suspectes liées aux rançongiciels sont probablement, et de manière générale, sous-déclarées dans tous les secteurs. Des problèmes de détection peuvent survenir en raison de la nature décentralisée de l'emplacement géographique des groupes criminels de rançongiciels, de la diversité de criminels impliqués et de l'utilisation de différentes techniques de blanchiment de capitaux. Aucun secteur n'est en mesure de contempler l'ensemble du tableau.

43. Pour améliorer la fréquence et la qualité des signalements par les entités réglementées, ainsi que la détection au sens plus large, les pays se sont appuyés sur diverses méthodes, telles que la participation du secteur privé et l'élaboration et l'échange d'indicateurs d'alerte et de guides de détection (consulter également la section 8.3 ci-dessous).

Encadré 10. Guide de l'Israel Money Laundering and Terror Financing Prohibition Authority (IMPA) sur les rançongiciels

La CRF d'Israël, IMPA, a mené une analyse stratégique des rapports d'activité inhabituels afin d'identifier les caractéristiques des paiements de rançongiciels. L'analyse comprenait des renseignements sur la fréquence d'attaques et le type d'entités visées, les sommes versées, les types d'actifs virtuels utilisés et l'implication de tiers. Un guide axé sur les rançongiciels a été publié à la suite de cette analyse. Le guide traitait des indicateurs d'alerte et des études de cas. Il a été publié sur le site Web de l'IMPA[1], puis il a été transmis avec un communiqué de presse officiel à toutes les entités déclarantes concernées.

Les résultats de la recherche ont également été présentés à diverses occasions lors de forums publics et de conférences professionnelles. La publication encourageait, entre autres, l'implication du secteur israélien de la réponse aux incidents, ouvrant ainsi la voie à l'élargissement de ces relations et à l'étude des possibilités de coopération et d'échange de renseignements ultérieures.

Source : Israël

1. En hébreu seulement : www.gov.il/BlobFolder/dynamiccollectorresultitem/red-flags-typology-ransomware-impa-140222/he/professional-docs_red_flags_typology_ransomware_impa_140222.pdf

44. Dans la plupart des cas où un PSAV dépose une déclaration de soupçons liée à un rançongiciel, celle-ci est déposée en raison d'un soupçon sur l'achat d'actifs virtuels qui serviraient à payer une rançon. Les indicateurs utiles sur lesquels les PSAV s'appuient comprennent les propres déclarations de la victime au PSAV, les achats effectués par une entreprise connue de réponse aux incidents, ainsi que les paiements effectués qui sont directement ou indirectement liés à une adresse d'actifs virtuels exposée à un rançongiciel qui a fort probablement été identifié grâce à une analyse de la chaîne de blocs. Puisque les PSAV agissent à titre

d'intermédiaire direct lors de nombreux paiements de rançon, ils sont une source clé de déclarations de soupçons sur les flux financiers illicites liés aux rançongiciels. Veuillez consulter le document « Lutte contre le financement des rançongiciels : indicateurs de risque » pour obtenir une liste des indicateurs de risque pertinents sur lesquels les PSAV peuvent s'appuyer.

Encadré 11. Intervention d'une entreprise de gestion de crise

L'IMPA a reçu une déclaration de soupçons de la part d'un PSAV israélien au sujet d'une entreprise de gestion de crise (réponse aux incidents) ayant acheté des actifs virtuels (évalués à des dizaines de milliers de dollars à l'époque) destinés au paiement d'un rançongiciel au nom d'une victime dont l'identité n'a pas été divulguée. Selon la déclaration de soupçons, un représentant de la cible présumée, provenant du même PSAV israélien, a également acheté, de manière indépendante, une quantité supplémentaire de cryptomonnaie.

L'enquête financière de l'IMPA a révélé que l'adresse du portefeuille qui recevait la plupart des fonds avait des liens avec d'autres attaques de rançongiciels et recevait des fonds d'autres adresses. Les fonds accumulés ont ensuite été transférés à un PSAV situé dans un État à haut risque. De plus, les fonds achetés indépendamment par l'entreprise ont été transférés à l'aide de plusieurs adresses. Une grande partie de ces fonds ont finalement été acheminés à l'aide de mélangeurs. Un bulletin de renseignement a été transmis aux AEP concernés dans le cadre d'une enquête plus approfondie.

Source : Israël

45. Contrairement aux PSAV, les banques et autres institutions financières et de paiement peuvent détecter une victime transférant de la monnaie fiduciaire à un PSAV ou à un tiers agissant en son nom dans le cadre d'un paiement de rançon, et peuvent, par conséquent, déposer une déclaration de soupçons. Il est toutefois possible que ces institutions n'aient pas un aperçu direct des paiements liés aux rançongiciels ou du blanchiment de capitaux connexe, car la plupart des paiements sont versés en actifs virtuels et non en monnaie fiduciaire. Par conséquent, ces institutions financières et de paiement peuvent disposer de renseignements très limités sur les adresses d'actifs virtuels ou la source des fonds, ce qui rend difficile pour elles l'utilisation de l'analyse de la chaîne de blocs. Pour atténuer ces défis, ces institutions ont souvent besoin d'indicateurs indirects pour identifier les paiements potentiels de rançongiciels. Selon les études de cas, les indicateurs courants comprennent les transferts inhabituels vers des PSAV (surtout lorsque l'entreprise n'exploite habituellement pas d'actifs virtuels), l'achat d'actifs virtuels par des entreprises de cybersécurité, des compagnies d'assurance et des entreprises d'intervention en cas d'incidents, les propres déclarations des clients qu'un transfert bancaire est utilisé pour payer une demande de rançon, ainsi que des renseignements de source ouverte corroborant l'attaque (des communiqués de presse ou des rapports d'incidents, par exemple). Le document « Lutte contre le financement des rançongiciels :

indicateurs de risque » contient une liste détaillée des indicateurs de risque pertinents.

Signalement par les victimes

46. En raison des faibles niveaux de signalement d'opérations suspectes pour les paiements de rançongiciels dans la plupart des pays, les déclarations de soupçons demeurent une source de détection insuffisante et ne permettent pas de comprendre l'ampleur intégrale des attaques de rançongiciels et du blanchiment de capitaux connexes ni de soutenir les enquêtes. Par conséquent, le signalement par les victimes est également une source importante de renseignements pour détecter les flux financiers liés aux rançongiciels et enquêter sur ceux-ci. Le signalement par les victimes en temps opportun est un élément crucial permettant aux AEP d'agir rapidement pour localiser les flux financiers et qui augmente la probabilité d'obtenir de bons résultats d'application.

47. Les exigences de signalement d'incident varient d'un pays à l'autre et dépendent du cadre juridique de chacun d'entre eux. Le signalement des incidents est volontaire pour la plupart des cas. Lorsque les victimes signalent un incident, elles contactent habituellement la police, les entreprises de cybersécurité, les unités spécialisées en signalement de cyberincidents ou les équipes locales d'intervention d'urgence informatique (CERT).

48. Le signalement par les victimes s'avère toutefois limité, car les attaques sont sous-déclarées. Il existe plusieurs raisons pouvant dissuader les victimes de signaler volontairement les attaques de rançongiciels, notamment la source de conflits potentiels contre leurs propres intérêts commerciaux. Parmi ces raisons, on compte les préoccupations concernant l'atteinte à la réputation, le désir de restaurer rapidement les activités ou la peur de représailles de la part des criminels. La nature des rançongiciels implique généralement un accès illicite aux données personnelles et délicates des clients. Avouer aux AEP ou au public qu'il existe une défaillance sur les plans de la sécurité et des données pourrait, selon certains, affecter les activités de l'entreprise et entraîner des poursuites au civil. Les criminels peuvent également menacer de divulguer les données de la victime au public si cette dernière contacte les AEP.

49. De plus, les victimes peuvent ne pas être incitées à signaler volontairement les incidents après le paiement de la rançon. Si la victime a souscrit à une cyberassurance, elle peut manquer de motivation financière pour signaler une attaque si la compagnie d'assurance couvre le coût du paiement. Dans certains pays, il est possible que les victimes ne se manifestent pas après avoir payé des rançons par crainte d'enfreindre les règlements nationaux (par exemple, les paiements versés à une entité sanctionnée) ou d'être considérées comme complices des groupes criminels.

50. Les pays ont adopté une série de méthodes pour encourager les victimes à signaler les attaques. Certains pays, par exemple, ont mis en œuvre des politiques ou mené des activités telles que des campagnes publiques pour sensibiliser la population aux attaques de rançongiciels et encourager le signalement des incidents. Ces politiques et activités impliquent généralement le secteur privé et servent à souligner la manière dont les autorités peuvent aider à atténuer l'incidence des attaques de rançongiciels. Cela comprend la restitution des actifs

aux victimes et la transmission des clés de déchiffrement pour récupérer les données, lorsqu'elles sont disponibles.

Encadré 12. No More Ransom [1]

Le site Web « No More Ransom » est une initiative de la National High Tech Crime Unit (unité nationale de lutte contre les crimes informatiques) des Pays-Bas, du Centre européen de lutte contre la cybercriminalité d'Europol et de deux partenaires industriels dans le but d'aider les victimes de rançongiciels à récupérer leurs données cryptées sans avoir à payer les criminels. Le site Web contient un référentiel de clés et d'applications capables de déchiffrer les données verrouillées par différents types de rançongiciels. Cet outil aide les victimes à restaurer leur accès à leurs fichiers cryptés ou à leurs systèmes verrouillés sans avoir à payer les rançons.

L'initiative regroupe de nombreux partenaires des secteurs public et privé de plusieurs pays, y compris des AEP et des entreprises de sécurité informatique. Cette initiative vise à informer les utilisateurs sur le fonctionnement des rançongiciels et sur les contre-mesures pouvant être prises pour prévenir efficacement l'infection. Le site Web encourage en outre les victimes à ne payer aucune rançon et fournit des liens pour rediriger les victimes vers le site Web de signalement de leur pays, afin de déposer une plainte au sujet d'un incident.

Source : No More Ransom

1. Pour de plus amples renseignements, consultez le site Web www.nomoreransom.org/en/index.html

51. Pour contrer les inquiétudes au sujet du risque d'atteinte à la réputation lié au signalement, certains pays ont tenté de créer un environnement sûr où les entreprises victimes d'attaques de rançongiciels peuvent se manifester sans craindre pour leur réputation, grâce à des interactions fréquentes et des conférences professionnelles, par exemple. Voici un autre exemple de pratique exemplaire : la création de portails de sites Web « à guichet unique » permettant aux victimes de signaler les incidents tout en servant de centre de ressources pour des conseils et des mesures correctives. Bien que ces efforts se concentrent souvent sur la détection de l'attaque par rançongiciel elle-même, les renseignements obtenus à partir d'un rapport de victime sont essentiels aux enquêtes financières, notamment la surveillance des flux financiers connexes et du blanchiment de capitaux.

Encadré 13. Centre canadien pour la cybersécurité

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) a été mis sur pied en 2018 en tant qu'initiative clé de la Stratégie nationale de cybersécurité du Canada. Il s'agit de la source unifiée de conseils, d'avis, de services et de soutien spécialisés en matière de cybersécurité pour le gouvernement, les propriétaires d'infrastructures essentielles et les activités de celles-ci, le secteur privé et le secteur public du Canada. Le Centre pour la cybersécurité offre des ressources aux particuliers et aux entreprises, notamment des conseils sur la manière de prévenir les incidents de rançongiciels et de s'en remettre, ainsi que des rapports sur le contexte de ces cybermenaces. Le Centre pour la cybersécurité recueille les rapports sur les cyberincidents des intervenants du gouvernement et du secteur privé à l'échelle nationale et mondiale. Il est possible de signaler un cyberincident en ligne par courriel ou par téléphone. Le Centre encourage également de contacter la police s'il juge qu'un cyberincident constitue un danger imminent pour la vie de la victime ou qu'il relève de la justice pénale.

Source : Canada

52. Certains pays ont adopté l'approche consistant à cibler certains secteurs ou cas dans lesquels le signalement par les victimes est obligatoire, par exemple, pour les attaques contre les infrastructures essentielles (telles que l'énergie, les communications, les soins de santé, etc.) ou les fuites de données. Dans de nombreux pays, ces industries peuvent également englober des secteurs financiers assujettis aux exigences de LBC-FT, comme les banques, où les entités réglementées sont tenues de signaler les incidents majeurs aux autorités compétentes, telles que les superviseurs, conformément au cadre réglementaire. Les cadres de protection des données peuvent encourager ou exiger le signalement obligatoire des violations de données impliquant des renseignements personnels, ce qui peut favoriser une détection rapide. Il est recommandé de recueillir les renseignements financiers pertinents lors de ces signalements, tels que l'adresse du portefeuille ou le type d'actif virtuel, afin d'améliorer la détection de flux financiers illicites.

Autres sources de détection

53. Comme nous l'avons susmentionné, les échanges et la collaboration avec des intervenants externes aux institutions financières, aux secteurs d'EPNFD et de PSAV, comme les fournisseurs de services Internet et le secteur de la cybersécurité, peuvent constituer une source potentielle de renseignements précieux. Ces secteurs peuvent toutefois ne pas être assujettis aux exigences réglementaires en matière de LBC-FT, y compris les déclarations de soupçons. Dans certains cas, il peut y avoir un conflit d'intérêts potentiel (par exemple, des entreprises de cybersécurité agissant au nom des victimes), ce qui pourrait limiter le signalement proactif. Dans de telles circonstances, les renseignements peuvent être obtenus au moyen de mécanismes informels tels que des

partenariats public ou privé impliquant ces entités, ou en interagissant directement avec celles-ci.

Encadré 14. Collaboration avec une entreprise de cybersécurité

Une entreprise victime a engagé une entreprise de cybersécurité après avoir subi une attaque d'un groupe de rançongiciels. Les criminels ont exigé une rançon en Bitcoin ou en Monero. La victime a finalement payé la rançon au groupe criminel par l'intermédiaire de l'entreprise de cybersécurité.

Cette dernière a par la suite informé les autorités de cet incident, ce qui a permis aux autorités de localiser les flux illicites. Les autorités collaborent fréquemment avec des entreprises de cybersécurité. Cette collaboration vise à réduire au minimum les interférences avec le travail des entreprises de cybersécurité pour la reprise des activités de leurs clients, tout en fournissant les éléments clés, comme les adresses IP et de cryptomonnaie, aux enquêtes criminelles.

Pour cette affaire, les forces de l'ordre ont observé l'utilisation de techniques d'anonymisation telles que les mélangeurs et l'emploi de nombreuses adresses de portefeuille non hébergées. Au moment de l'enquête, une partie importante des actifs était conservée dans des portefeuilles non hébergés et ne pouvait donc pas être localisée avec exactitude. La majeure partie des fonds aurait été acheminée par l'intermédiaire de deux PSAV situés dans des États étrangers.

Source : Suisse

54. Les autorités compétentes détectent également les attaques de rançongiciels et les paiements au moyen d'enquêtes financières indépendantes utilisant l'analyse de la chaîne de blocs sur les portefeuilles connus pour établir des liens avec les rançongiciels. Il s'agit alors de surveiller les attaques connues, les blogs et les analyses de sources ouvertes partagées par les sociétés d'analyse de la blockchain ainsi que d'établir un contact proactif avec les victimes potentielles après analyse.

55. Ces efforts peuvent révéler des pistes supplémentaires vers des attaques de rançongiciels antérieures. Ils peuvent également donner des indications sur l'ampleur d'une attaque imputable à un criminel utilisant un rançongiciel, ainsi que sur les tendances, les typologies et l'infrastructure que les criminels utilisent pour blanchir, recevoir et utiliser leurs produits illicites.

Encadré 15. Analyse des sources ouvertes pour identifier les criminels de RaaS

La CRF turque a reçu une déclaration de soupçons de la part d'un PSAV concernant une adresse de portefeuille d'actifs virtuels liée à une personne enregistrée sous le nom de « Nom 1 » par le PSAV. Une recherche en ligne du nom a révélé un site Web du même nom. Une enquête plus approfondie a montré que le site Web menait des activités liées à l'Internet clandestin et servait d'intermédiaire dans la vente de rançongiciels et d'autres logiciels malveillants.

Une analyse plus approfondie sur les sources ouvertes a révélé que :

- La personne impliquée dans l'opération mentionnée dans la déclaration de soupçons a utilisé un pseudonyme différent (« Nom 2 »). Cette révélation a permis de découvrir la véritable identité de cette personne (« Personne X »). Cette personne était auparavant une personne d'intérêt de la direction de lutte contre la cybercriminalité du service de police turc.
- Le suspect (Personne X) offrait des services et des produits tels que l'accès non autorisé, l'accès à des renseignements confidentiels, de fausses pièces d'identité, le piratage de comptes de médias sociaux, ainsi que la vente de liens de piratage et de pages d'hameçonnage.
- Les paiements pour ces produits et services illégaux ont été versés en Bitcoin et d'autres actifs virtuels.

La CRF de la Turquie a ensuite demandé des renseignements supplémentaires au PSAV au sujet de la personne mentionnée dans la déclaration de soupçons, plus précisément les adresses de portefeuille d'actifs virtuels, les opérations financières (actifs virtuels et monnaie fiduciaire) et d'autres renseignements personnels. Un rapport d'analyse a été préparé et soumis aux départements de la cybercriminalité de la police nationale turque. Le rapport soupçonne que la personne mentionnée dans la déclaration de soupçons était un intermédiaire dans la vente de rançongiciels et d'autres logiciels malveillants. Des enquêtes sont en cours.

Source : Turquie

56. Les pays peuvent être alertés des attaques de rançongiciels et des paiements grâce aux renseignements fournis par les autres pays. La coopération internationale, l'entraide judiciaire et l'échange informel de renseignements avec d'autres pays peuvent fournir des renseignements sur les fonds empilés au moyen d'échanges nationaux liés à des attaques et à des victimes étrangères.

Mesures proposées

- Les États devraient prêter main-forte aux entités réglementées dans la détection de rançongiciels et du blanchiment de capitaux connexe et dans le signalement d'opérations suspectes, notamment en communiquant les tendances, les guides de détection et les indicateurs d'alerte (comme ceux contenus dans « Lutte contre le financement des rançongiciels : indicateurs de risque ») aux entités déclarantes concernées.
- Les États devraient encourager les victimes à signaler volontairement les incidents, par exemple en les sensibilisant au soutien et aux ressources disponibles ou en créant des canaux sûrs de signalement.
- Les États devraient envisager d'établir des canaux de communication avec des acteurs non traditionnels qui peuvent ne pas être soumis aux exigences de LBC-FT (comme les entreprises de cyberassurance et de réponse aux incidents), afin d'augmenter les sources de détection.

Stratégies d'enquête financière

57. L'objectif de presque toutes les attaques de rançongiciels est de générer des profits. La plupart des pays reconnaissent que les enquêtes sur les rançongiciels comportent un volet financier important. Des études de cas montrent que la localisation des actifs virtuels est un élément clé des enquêtes sur les rançongiciels. En ce qui concerne les pays affirmant mener des enquêtes sur les attaques de rançongiciels, ces derniers mènent habituellement des enquêtes financières en parallèle afin de localiser le paiement de la rançon.

58. Dans l'ensemble, on dénote un manque d'expérience en matière d'enquêtes sur le blanchiment de capitaux lié aux rançongiciels. Très peu de pays ont porté des accusations de blanchiment de capitaux dans des affaires de rançongiciels. Cette situation peut être en partie attribuable aux difficultés de détection et de signalement, comme nous en avons discuté à la section 5 précédente.

59. Cette section examine les défis spécifiques et les pratiques exemplaires liés à la réussite des enquêtes financières sur les rançongiciels et le blanchiment de capitaux connexe, notamment (i) la collaboration avec les victimes pour accéder aux renseignements; (ii) les techniques et mécanismes d'enquête; (iii) le recouvrement d'actifs.

Mesures rapides et collaboration avec les victimes pour accéder aux renseignements

60. Compte tenu de la nature des cybercrimes tels que les rançongiciels, les résultats fructueux d'application de la loi dépendent de la capacité à agir rapidement et à recueillir des renseignements clés liés à l'attaque et au paiement du rançongiciel. Ces renseignements comprennent les adresses des actifs virtuels, la somme totale de la rançon et le type d'actif virtuel utilisé, les dates des transferts, les

types de services impliqués, l'identité de la victime, les communications entre la victime et les criminels derrière les rançongiciels, ainsi que tout tiers impliqué dans le paiement de la rançon.

61. La collecte de ces renseignements dépend bien souvent de la coopération des victimes ou de tiers impliqués dans la réponse à l'incident ou le processus de paiement de la rançon. Cependant, comme nous l'avons déjà mentionné, les victimes peuvent être réticentes à signaler les incidents aux forces de l'ordre (consulter la section 5.3 ci-dessus). Les victimes peuvent également être réticentes à coopérer en raison de conflits d'intérêts perçus avec les forces de l'ordre. Les victimes souhaitent souvent reprendre les activités commerciales dès que possible et peuvent préférer payer la rançon. De plus, si elles communiquent avec les autorités, elles peuvent craindre les représailles des criminels. Les forces de l'ordre, quant à elles, peuvent avoir besoin de temps pour obtenir des preuves médicolégales, mettre sur pied des opérations contrôlées et prendre d'autres mesures d'enquête, ce qui peut retarder la reprise des services.

62. Un signalement tardif ou incomplet et le manque de coopération des victimes peuvent compromettre la qualité des renseignements obtenus pour poursuivre et approfondir efficacement les enquêtes. Si les victimes n'ont pas un plan d'action clair à entreprendre après une attaque ou un paiement, il est possible que les preuves obtenues soient compromises en raison de l'absence de conservation des données. Les pratiques exemplaires abordées dans la section 5.3, telles que les campagnes publiques et d'autres efforts pour encourager la coopération des victimes, sont importantes pour atténuer ces défis.

63. Certains pays ont en outre souligné l'importance de l'échange de renseignements entre les cyberenquêteurs (prédicats) et les enquêteurs chargés du blanchiment de capitaux. Pendant qu'elles recueillent des preuves médicolégales dans le cadre de l'enquête préalable sur les rançongiciels, les forces de l'ordre recueilleront inévitablement des renseignements pertinents pour l'enquête sur le blanchiment de capitaux. De tels renseignements permettent aux forces de l'ordre d'établir des liens entre différents groupes et affiliés d'attaquants utilisant des rançongiciels, en plus de fournir des pistes de suivi pour soutenir une enquête financière plus large. Pour en connaître davantage sur la manière dont les différentes autorités compétentes nationales peuvent coopérer efficacement, veuillez consulter la section 8.2 ci-après.

Encadré 16. Sources de preuves pertinentes pour les enquêtes financières obtenues lors d'enquêtes préalables

Preuves médicolégales : des exemples de preuves médicolégales comprennent les vecteurs d'attaque (c'est-à-dire comment les criminels obtiennent un accès non autorisé), des renseignements sur le type de rançongiciel, les adresses IP, les noms ou pseudonymes utilisés, ainsi que les appareils de l'attaquant. Ces renseignements peuvent être obtenus directement auprès des victimes, des fournisseurs de services Internet, des entreprises de cybersécurité et d'intervention en cas d'incidents et grâce aux technologies médicolégales.

Preuve directe provenant du secteur privé : les entreprises du secteur privé concernées comprennent les entreprises possédant la technologie ou l'infrastructure qui a été utilisée à mauvais escient lors d'une attaque par rançongiciel. Les enquêteurs peuvent obtenir des renseignements sur les abonnés par courriel ou par l'intermédiaire d'entreprises de médias sociaux auprès desquelles l'auteur du crime peut avoir détenu des comptes pour communiquer avec la victime.

Renseignements provenant de sources ouvertes : l'examen des renseignements provenant de sources ouvertes, notamment les médias sociaux, les forums en ligne, les marchés de l'Internet clandestin et les communications des criminels utilisant des rançongiciels, peut aider à identifier les auteurs potentiels de cybercrimes.

Techniques et mécanismes d'enquête

Pertinence des techniques d'enquête traditionnelles

64. Les technologies utilisées par les criminels derrière les rançongiciels pour dissimuler leur emplacement, leur identité et leurs flux financiers peuvent entraver les enquêtes. Les défis spécifiques comprennent l'utilisation de RPV, « The Onion Router [35] » ou de courriels cryptés pour permettre une confidentialité et une sécurité accrues, ainsi qu'une activité sous le couvert de l'anonymat lorsque le trafic se déplace dans un réseau. Ces défis peuvent être aggravés en raison de la vitesse à laquelle ces technologies évoluent.

65. La recommandation 31 du GAFI jette les bases pour conférer aux AEP les pouvoirs nécessaires pour mener des enquêtes financières efficaces. Ces techniques d'enquête traditionnelles demeurent pertinentes pour surmonter ces défis, afin de permettre la collecte et l'analyse de renseignements clés liés aux flux financiers découlant de rançongiciels. Cela comprend la surveillance, l'interception des communications ainsi que les opérations d'infiltration. Ces techniques traditionnelles devront cependant être adaptées dans le cadre d'enquêtes financières impliquant des actifs virtuels. Voici quelques exemples démontrant comment obtenir des résultats d'enquête fructueux :

- *Surveillance* : déterminer les types d'appareils électroniques qu'un suspect utilise, pour détecter les portefeuilles virtuels utilisés ainsi que leurs méthodes préférées de communication électronique.
- *Intercepter les communications et opérations d'infiltration* : obtenir des renseignements sur les activités du sujet et le fonctionnement d'une organisation criminelle, identifier les individus affiliés au sujet, obtenir des renseignements financiers et des renseignements sur les actifs pertinents, ainsi qu'infiltrer des communautés criminelles (comme les forums de l'Internet clandestin) pour identifier les auteurs et les bénéficiaires véritables.
- *Ordonnances de communication :* obtenir des renseignements auprès de PSAV ou d'autres institutions financières impliquées dans le paiement de rançons, etc.

66. L'utilisation de ces outils dans les enquêtes financières peut être étayée par des renseignements obtenus par une déclaration de soupçons ou grâce aux signalements par les victimes (consulter la section 5 ci-dessus). Les forces de l'ordre peuvent délivrer une ordonnance de communication dans le but d'obtenir les preuves nécessaires à l'identification des institutions financières et des PSAV concernés, et ce, au moyen de déclarations de soupçons ou d'analyses de chaînes de blocs (consulter la section 6.2.2 ci-dessous). Les PSAV peuvent fournir des renseignements d'identification utiles au soutien des enquêtes financières sur les rançongiciels, afin d'obtenir des renseignements fondamentaux et des renseignements sur la propriété effective et les opérations (comme l'identité de l'utilisateur et les renseignements connexes, les adresses IP, les cartes de crédit ou les comptes bancaires, etc.).

67. Cependant, comme le mentionne la section 3 précédente, certains réseaux de rançongiciels ont également été liés à des pays à haut risque où les exigences en

[35] Également connu sous le nom de TOR, il s'agit d'un logiciel de source ouverte qui permet aux utilisateurs de naviguer sur Internet de manière anonyme.

matière de LBC-FT pour les PSAV sont faibles ou inexistantes, ou dans lesquels les PSAV satisfont rarement aux exigences. Par conséquent, les enquêtes peuvent se corser si les fonds transitent par ces PSAV ou sont détenus par ces derniers. Dans de tels cas, il est possible que les PSAV ne recueillent pas du tout les renseignements pertinents ou qu'ils ne répondent pas aux demandes des autorités.

68. Les enquêteurs sont confrontés à des défis semblables lorsque les criminels utilisent des portefeuilles non hébergés. Cela permet aux utilisateurs de contrôler les actifs virtuels sans l'implication d'un PSAV, ce qui soulève des défis pour détecter et prévenir les activités de blanchiment de capitaux. L'absence de lien avec une entité tierce (qui devrait être enregistrée ou licenciée, selon les normes du GAFI) peut compliquer la capacité des autorités à identifier le propriétaire du portefeuille, car il n'y a pas de partie externe auprès de laquelle on peut obtenir des renseignements.

69. La mise en œuvre limitée de la « règle d'acheminement » du GAFI par les PSAV offre également aux cybercriminels la possibilité d'éviter d'être détectés et d'entraver les enquêtes. La règle d'acheminement exige que les PSAV et les autres institutions financières effectuant des transferts d'actifs virtuels communiquent des renseignements sur l'expéditeur (donneur d'ordre) et le destinataire (bénéficiaire) lors de tout transfert. Cette mesure augmente la transparence des opérations pour prévenir les abus criminels et constitue une source de renseignements auxquels les forces de l'ordre peuvent accéder pour identifier les parties impliquées dans une opération donnée. Cependant, un rapport du GAFI de 2022 a révélé que seulement un tiers des pays affirment avoir adopté des lois pour imposer la règle d'acheminement aux PSAV, et qu'encore moins se conforment réellement à ces exigences[36]. Ce manque de réglementation cohérente réduit la quantité de renseignements que les PSAV peuvent mettre à la disposition des autorités dans les pays n'étant pas assujettis à la règle d'acheminement. Cela signifie également que les PSAV de pays conformes effectuant des opérations avec les PSAV de pays non conformes ne seront probablement pas en mesure d'obtenir ces renseignements, ce qui limitera l'information mise à la disposition des enquêteurs, et ce, même dans les pays appliquant la règle d'acheminement.

[36] GAFI (juin 2022) *Targeted Update on Implementation of FATF's Standards on VAs and VASPs*, en anglais seulement. La mise à jour ciblée ne couvre que les pays dont les rapports d'évaluation mutuelle et les rapports de suivi ont été publiés entre juin 2021 et mai 2022.

Encadré 17. Techniques d'enquête traditionnelles et financières sur un groupe utilisant des rançongiciels

Une entreprise italienne victime d'une attaque a déposé une plainte auprès de la police après avoir effectué un paiement de rançon en Bitcoin et réussi à déverrouiller ses données infectées par le rançongiciel. Le paiement a été effectué par l'intermédiaire d'un PSAV mentionné dans la demande de rançon.

Les enquêtes policières sur le PSAV ont révélé que son site Web était officiellement enregistré en Italie. Un sujet italien a par la suite été identifié. Les autorités ont découvert que le sujet a facilité les flux de Bitcoin liés au paiement de la rançon. La police a perquisitionné son appartement et saisi des cartes de paiement, des téléphones portables, ainsi que du matériel informatique, comme des disques durs, des clés USB et des tablettes. Les écoutes téléphoniques et l'analyse des messages échangés sur les téléphones portables ont permis d'identifier un groupe d'autres sujets italiens (le « Groupe ») ayant joué des rôles similaires en facilitant les flux de Bitcoin liés aux rançongiciels. Les enquêtes financières ont révélé que les fonds fiduciaires envoyés par les victimes du rançongiciel avaient été transférés par le Groupe sur des comptes bancaires étrangers gérés par des PSAV étrangers, notamment des PSAV situés dans des pays à haut risque.

Selon des enquêtes financières et une analyse médicolégale des téléphones et du matériel informatique, les autorités ont conclu que le Groupe diffusait des rançongiciels dont les rançons s'élevaient à plusieurs centaines d'euros par attaque. Le Groupe a été accusé d'extorsion liée à un rançongiciel et du blanchiment subséquent des produits, estimés à environ 300 000 euros répartis entre plusieurs victimes. Les enquêtes sont toujours en cours.

Source : Italie

Techniques propres aux actifs virtuels

70. En plus des techniques traditionnelles, les forces de l'ordre devraient s'appuyer sur des techniques propres aux actifs virtuels pour mener des enquêtes financières sur les rançongiciels. La plupart des actifs virtuels sont exploités sur une chaîne de blocs publique, qui agit comme une base de données consultable où il est possible de localiser des renseignements pseudonymes liés aux opérations d'actifs virtuels au moyen d'outils de sources ouvertes ou d'analyse d'abonnements aux chaînes de blocs (consulter la section 7 ci-dessous). L'analyse de la chaîne de blocs, combinée aux techniques d'enquête traditionnelles, peut permettre aux enquêteurs d'obtenir les renseignements nécessaires pour identifier les criminels utilisant des rançongiciels et leurs affiliés, ainsi que de suivre le mouvement des produits illicites.

71. La détection et la collecte de renseignements sur le paiement d'une rançon sont une première étape essentielle à la localisation des produits au moyen d'une analyse de la chaîne de blocs, car il faut généralement cerner une adresse de portefeuille initiale pour lancer cette analyse. Une fois qu'une adresse de

portefeuille initiale est fournie, les enquêteurs peuvent, entre autres, identifier les paiements effectués et reçus par cette adresse de portefeuille. Les renseignements à leur disposition peuvent toutefois dépendre du service utilisé. Bien que la chaîne de blocs publique contienne des renseignements utiles pour les enquêtes financières, certaines opérations d'actifs virtuels se produisent également hors chaîne. Certaines analyses de chaînes de blocs s'appuient en outre sur des algorithmes d'agglomération et d'autres techniques pour regrouper les adresses de portefeuille ou les opérations pouvant être associées à la criminalité, comme les rançongiciels.

72. Les renseignements obtenus par l'analyse de la chaîne de blocs peuvent éclairer davantage l'utilisation des techniques d'enquête traditionnelles. Par exemple, l'analyse de la chaîne de blocs pourrait aider à identifier un PSAV hébergeant une adresse de portefeuille qui a reçu un paiement envoyé à ou par des criminels utilisant des rançongiciels, ce qui pourrait inciter les AEP à utiliser des méthodes obligatoires pour demander des renseignements sur l'adresse du portefeuille du PSAV en question.

Encadré 18. Enquêtes sur des portefeuilles de rançongiciels connus révélant d'autres victimes inconnues

Une analyse en ligne des menaces contre la chaîne de blocs était en cours au sujet d'une adresse Bitcoin qui était connue pour avoir reçu environ 20 bitcoins entre le 12 mai 2017 et le 27 mai 2021. Il a été découvert que ladite adresse Bitcoin pourrait être directement liée à un rançongiciel ayant infecté plusieurs entités commerciales et ministères gouvernementaux en Afrique du Sud. L'analyse a révélé qu'une adresse Bitcoin locale distincte, qui appartenait à un PSAV en Afrique du Sud, avait fourni 0,06 bitcoin à l'adresse susmentionnée faisant l'objet d'une enquête en février 2018.

Une victime a été identifiée après avoir obtenu des renseignements d'abonnement auprès du PSAV. La victime a reconnu avoir subi un préjudice financier. La victime a préféré ne pas signaler l'incident aux autorités d'enquête locales, car elle craignait l'embarras public pour une mauvaise sécurisation des données des clients. La CRF d'Afrique du Sud a acheminé cette affaire aux autorités d'enquête locales. Puisque la victime identifiée ne voulait pas porter d'accusations criminelles, l'affaire a été retirée et classée par les forces de l'ordre locales.

Source : Afrique du Sud

73. Les méthodes de blanchiment renforçant l'anonymat utilisées par les criminels derrière les rançongiciels (abordées dans la section 3 précédente) donnent également du fil à retordre aux autorités chargées de l'application de la loi pour localiser et attribuer les opérations à l'aide de l'analyse de la chaîne de blocs, bien que certaines entreprises spécialistes en la matière aient développé une technologie pour atténuer certaines de ces mesures. Les modèles d'affiliation ou les fournisseurs de RaaS, ainsi que l'implication de mules financières, viennent eux aussi complexifier les enquêtes financières liées aux rançongiciels. Étant

donné que les paiements ne peuvent pas toujours mener jusqu'à la victime, il devient difficile d'identifier les adresses utilisées pour le paiement initial des actifs virtuels, qui servent généralement de piste pour l'analyse de la chaîne de blocs.

74. Au-delà de l'utilisation de l'analyse de la chaîne de blocs pour remonter à la source du paiement de l'attaque par rançongiciels et de son blanchiment ultérieur, les enquêteurs doivent également localiser les opérations antérieures liées au groupe utilisant des rançongiciels. Cette étape supplémentaire permet aux forces de l'ordre de déterminer les tendances et typologies potentielles et/ou d'autres formes de criminalité.

75. À titre de pratique exemplaire, les autorités chargées de l'application de la loi de certains pays ont créé des bases de données regroupant des renseignements clés sur les mules ou les adresses de portefeuille impliquées dans les affaires de rançongiciels. Ces bases de données comprennent généralement des données sur les incidents, les renseignements d'identification des mules, l'ampleur des dommages et des renseignements sur les criminels utilisant des rançongiciels (par exemple, numéro de compte, adresses de portefeuille, noms d'utilisateur). Ces bases de données aident à cerner et à localiser les paiements de rançongiciels et le blanchiment de capitaux connexe en fournissant un référentiel pour coupler les pistes d'enquêtes antérieures (y compris les renseignements de paiement) aux incidents actuels et ultérieurs. Cela permet aux forces de l'ordre de comprendre le réseau de blanchiment plus large qui peut se faufiler dans diverses entités et secteurs réglementés.

Recouvrement d'actifs

76. En plus du renforcement des capacités de détection et d'enquête financière, les autorités chargées de l'application des lois ont également besoin des pouvoirs législatifs et de la capacité de saisir et de confisquer les actifs virtuels. Les opérations d'actifs virtuels sont quasi instantanées. Cela signifie que dès que les autorités compétentes sont informées d'une attaque par rançongiciel et du paiement d'une rançon, elles doivent pouvoir localiser rapidement le paiement de la rançon et avoir accès à des pouvoirs de gel rapide, idéalement en quelques heures, pour éviter la dispersion des fonds. Conformément à la recommandation 4 du GAFI, de tels pouvoirs devraient déjà exister dans de nombreux pays, mais leur forme peut varier.

77. Plusieurs pays ont souligné l'utilité d'outils de rechange pour intercepter les produits illicites, tels que les pouvoirs de report des CRF, dans le traitement d'actifs possiblement criminels mentionnés dans les déclarations de soupçons. Pour suivre le rythme dynamique des actifs virtuels, il peut également être nécessaire d'envisager de mettre à jour les lois, les règlements, les politiques et les procédures existantes en matière de confiscation d'actifs.

Encadré 19. Colonial Pipeline

En juin 2021, le ministère américain de la Justice a annoncé avoir saisi 63,7 bitcoins d'une valeur d'environ 2,3 millions de dollars. Ces fonds seraient le produit du paiement de la rançon du 8 mai 2021 à des individus d'un groupe connu sous le nom de DarkSide qui avait ciblé Colonial Pipeline. L'attaque avait entraîné la mise hors service d'infrastructures essentielles. Un juge de la Californie a rendu une ordonnance de saisie plus tôt cette journée-là.

Vers le 7 mai 2021, Colonial Pipeline a été victime d'une attaque de rançongiciel très médiatisée, entraînant la mise hors service de certaines parties de son infrastructure. Colonial Pipeline a signalé au FBI que son réseau informatique avait été infiltré par une organisation du nom de DarkSide. L'entreprise aurait reçu une demande de rançon d'environ 75 bitcoins, demande qu'elle aurait payée. Selon les faits allégués dans l'affidavit à l'appui et en examinant le grand livre public de Bitcoin, les forces de l'ordre ont pu localiser plusieurs transferts de Bitcoins et déterminer qu'environ 63,7 bitcoins, soit le produit du paiement de la rançon, avaient été transférés à une adresse précise. Cette somme représente le produit dont la piste remonte à un piratage informatique et d'un bien impliqué dans le blanchiment de capitaux. Elle peut être saisie en vertu des lois pénales et civiles sur la confiscation.

Source : États-Unis

Mesures proposées

- Les autorités compétentes devraient utiliser et adapter, au besoin, les techniques d'application de la loi traditionnelles, ainsi que les techniques propres aux actifs virtuels, pour mener des enquêtes sur le blanchiment de capitaux liés aux rançongiciels.
- Les États devraient veiller à ce que les autorités de poursuite pénale disposent des capacités et des pouvoirs nécessaires pour saisir et confisquer rapidement et efficacement les actifs, en particulier les avoirs virtuels, et à ce que les autorités conservent ces capacités et pouvoirs.

Compétences et expertise

78. Comme l'indique la section 6.2, bien que les techniques traditionnelles d'application de la loi demeurent essentielles dans le cadre d'enquêtes sur le blanchiment de capitaux liées aux rançongiciels, une expertise technique spécialisée est toute de même requise pour mener à bien les enquêtes et les poursuites en matière de blanchiment de capitaux, ainsi que le recouvrement des actifs liés aux actifs virtuels. Cela comprend des connaissances technologiques et juridiques de l'écosystème des actifs virtuels.

79. De plus, les équipes d'enquête travaillant sur des cas de blanchiment de capitaux ou de recouvrement d'actifs liés à des rançongiciels doivent impliquer du personnel possédant des compétences techniques en cybersécurité et en criminalistique informatique, ainsi que des connaissances du monde numérique et des plateformes de sources ouvertes. Ces équipes devraient mettre l'accent sur la reconnaissance en ligne pour recueillir des renseignements financiers relatifs aux opérations d'actifs virtuels dans le domaine public, notamment des renseignements qui peuvent être obtenus par l'analyse de la chaîne de blocs, des sites Web, des médias sociaux, des forums en ligne, de l'Internet clandestin et des marchés noirs, ainsi que des renseignements tirés de rapports d'attaques en ligne.

80. Les autorités compétentes peuvent avoir besoin de nouvelles compétences et expertises pour interpréter et accéder aux renseignements, surtout si des actifs virtuels sont en jeu. Plus précisément, les autorités doivent se familiariser avec les capacités d'analyse et de surveillance de la chaîne de blocs, telles que l'utilisation d'outils d'analyse de la chaîne de blocs, les logiciels gratuits pour afficher les chaînes de blocs publiques, et les analyses pour localiser des fonds. De plus, différents outils offrent des fonctionnalités variées et complémentaires (analyse de différents types d'actifs virtuels, capacité d'analyser le saut de chaîne, renseignements puisés dans des sources ouvertes, etc.).

81. Une formation spécialisée et une expertise technique sont nécessaires pour développer ces divers outils et les utiliser lors des enquêtes. Certains pays ont ciblé des moyens d'impliquer des spécialistes lors d'enquêtes pertinentes (consulter la section 8.2). L'accès aux ressources requises peut être onéreux, et certains pays peuvent ne pas disposer des ressources nécessaires pour soutenir le perfectionnement de ces compétences, ce qui peut entraver la capacité des autorités à pourchasser les activités de blanchiment de capitaux liées aux rançongiciels.

82. Si les experts internes ne sont pas disponibles ou sont en nombre insuffisant, les pays peuvent envisager d'utiliser des outils créés par des entreprises du secteur privé. Des outils tiers peuvent aider les autorités à localiser, tracer et attribuer les opérations d'actifs virtuels sur toutes les chaînes de blocs d'actifs virtuels majeures et la plupart des chaînes mineures. À l'heure actuelle, ces outils prennent en charge des centaines de jetons et utilisent des méthodes telles que les algorithmes d'agglomération, le moissonnage (*Web scraping*) et la surveillance des bases de données frauduleuses qui permettent à un enquêteur de lier et d'attribuer un large éventail d'opérations à des individus et entités du monde réel. Les outils génèrent des graphiques d'opérations et permettent une analyse de réseau. Les entreprises peuvent ainsi comprendre les liens complexes et les présenter aux jurys et aux tribunaux lors de poursuites ultérieures et de

mesures de recouvrement d'actifs. Ces outils peuvent également aider les autorités à identifier les PSAV susceptibles d'avoir été utilisés pour blanchir ou échanger des produits illicites contre de la monnaie fiduciaire et qui pourraient disposer de renseignements pertinents pour étayer l'enquête.

83. En ce qui concerne le recouvrement d'actifs, la saisie et la gestion des actifs virtuels nécessitent une expertise technique et juridique supplémentaire. Les autorités doivent être prêtes à prendre les mesures appropriées et à mettre en œuvre des procédures pour assurer une saisie et un stockage appropriés. Le fait d'établir des mécanismes spécialisés de saisie, de confiscation et d'élimination des actifs virtuels est une pratique exemplaire. Cette pratique peut comprendre une bonne planification des saisies, la gestion des phrases secrètes (*seed phrases*[37]) et le stockage hors ligne (*cold storage*) des actifs virtuels saisis (c'est-à-dire leur stockage dans un portefeuille hors ligne non hébergé), ainsi que des problèmes de chaîne de possession.

Mesures proposées

- Les autorités compétentes devraient disposer des compétences spécialisées et de l'expertise nécessaires pour mener à bien les enquêtes financières relatives aux rançongiciels. Cela comprend la création d'analyses de chaînes de blocs et d'outils de surveillance, l'accès à ceux-ci, ainsi que la formation à cet égard.
- Les États devraient s'assurer que des mécanismes spécialisés sont en place pour gérer les actifs virtuels saisis de manière convenable.

Politiques nationales et coordination

Évaluation et stratégie nationales

84. La recommandation 1 du GAFI exige que les pays déterminent et évaluent leurs risques de blanchiment de capitaux et appliquent une approche fondée sur les risques pour atténuer ces derniers. Cette approche devrait également servir de base aux pays pour allouer efficacement les ressources dans leur régime de LBC-FT.

85. Les rançongiciels sont souvent abordés dans le cadre d'évaluations des menaces de cybersécurité. Par exemple, au niveau national, certaines juridictions ont adopté des stratégies nationales en matière de cybersécurité ou de cybercriminalité, qui soutienne la coordination nationale et fournissent l'engagement politique nécessaire pour lutter active contre les rançongiciels et les flux financiers illicites associés. Les stratégies nationales impliquent

[37] Les phrases secrètes sont un ensemble de mots générés aléatoirement par une application de portefeuille et répertoriés dans un ordre précis. Cet ensemble de mots peut être utilisé pour récupérer ou accéder à ses clés privées en contournant une protection supplémentaire (comme un mot de passe).

généralement divers organismes gouvernementaux[38] et peuvent impliquer les autorités compétentes en matière de LBC-FT telles que les ministères de la Justice, des Finances et de l'Intérieur, ainsi que le secteur privé. Cependant, il convient de noter que l'objectif de bon nombre de ces stratégies n'est pas nécessairement axé sur les risques de financement illicite, qui doivent être examinés en détail dans le cadre d'une évaluation des risques.

Encadré 20. Stratégie nationale de cybersécurité de l'Espagne

La stratégie nationale de cybersécurité de l'Espagne (dernière mise à jour en 2019) vise à renforcer les compétences pour lutter contre les cybermenaces. Elle définit les priorités, les objectifs et les mesures appropriées pour atteindre et maintenir un haut niveau de sécurité des réseaux et des systèmes d'information. Certaines des principales lignes de suivi de la stratégie visent à renforcer les compétences pour lutter contre les cybermenaces et à renforcer les capacités d'enquêter et de poursuivre les cybercrimes.

La stratégie a établi la nécessité de renforcer la coopération judiciaire et policière, tout en allouant des ressources suffisantes aux organismes compétents et en fournissant une formation professionnelle. Ceci est également lié à la création d'un cadre institutionnel pour la cybersécurité, ce qui a donné lieu au Conseil national de la cybersécurité. Ce Conseil est dirigé par le premier ministre espagnol dans le but de coordonner la politique de sécurité nationale en matière de cybersécurité et de promouvoir la coordination, la collaboration et la coopération entre les organismes d'administration publiques[1] et le secteur privé[2]. Le Conseil joue un rôle important dans l'approche multidisciplinaire.

Source : Espagne

Notes
1. Ministères des Affaires étrangères, de la Justice, de la Défense, de l'Intérieur, du Trésor, de la Présidence; le Centre national de renseignement, le Département de la sécurité nationale et d'autres.
2. Les experts du secteur privé comprennent ceux des associations professionnelles, des entreprises et des universités.

86. Conformément à la recommandation 1 du GAFI, les pays doivent s'assurer de tenir compte de la menace posée par les rançongiciels dans le cadre de leur évaluation nationale des risques de blanchiment de capitaux. Cette évaluation jette les bases à partir desquelles les pays peuvent élaborer des mesures d'atténuation, notamment la mise en œuvre des mesures suggérées dans le présent rapport. Avec une bonne compréhension des risques de blanchiment de capitaux liés aux rançongiciels, les pays seront en mesure d'allouer des

[38] Ces organismes comprennent ceux qui se concentrent sur l'application de la loi, la défense, la sécurité et la communication d'information, compte tenu de la menace pour la sécurité nationale posée par les rançongiciels.

ressources selon une approche fondée sur les risques, notamment pour acquérir des compétences et une expertise techniques en matière d'actifs virtuels et des outils d'analyse de chaîne de blocs au sein des autorités compétentes en matière de LBC-FT.

87. Les pays où les rançongiciels et le blanchiment de capitaux connexe ne constituent pas actuellement une menace nationale importante doivent également tenir compte des risques de financement illicite posés par les rançongiciels, plus précisément en raison de la relation unique entre les rançongiciels et les actifs virtuels. Les pays doivent non seulement tenir compte de la menace d'attaques de rançongiciels contre les victimes nationales, mais également de la possibilité que des criminels utilisant de tels logiciels soient basés en leur sein. Ils doivent également tenir compte de la possibilité que des PSAV locaux soient utilisés pour blanchir ou encaisser les produits des rançongiciels. Par exemple, les architectures de nombreux PSAV peuvent être réparties dans plusieurs pays. Un PSAV pourrait être enregistré auprès d'un pays donné, mais le personnel travaillerait à partir d'un autre pays. Les PSAV peuvent également héberger leurs infrastructures techniques et leurs clés privées dans des pays différents. Cela signifie que ces pays pourraient toujours être exposés aux mouvements financiers illicites liés aux rançongiciels, notamment par le secteur des PSAV.

Encadré 21. Évaluation des rançongiciels dans les évaluations nationales des risques de blanchiment de capitaux

En mars 2022, les États-Unis ont publié leur troisième évaluation nationale des risques de blanchiment de capitaux (NMLRA), qui met en évidence les menaces financières illicites les plus importantes, notamment la cybercriminalité ainsi que les vulnérabilités liées aux actifs virtuels. La NMLRA a déterminé que les incidents de cybercriminalité ont considérablement augmenté depuis 2018 et que les rançongiciels présentent une menace financière illicite particulièrement importante. La NMLRA a constaté, par exemple, que la gravité et la complexité des attaques de rançongiciels se sont accrues pendant la pandémie de la COVID-19. La NMLRA fournit d'importants renseignements sur les tendances des attaques de rançongiciels, notamment l'utilisation des rançongiciels en tant que modèle de service et les tactiques de double extorsion. La NMLRA met également en évidence de nombreuses typologies de blanchiment de capitaux, telles que l'utilisation de PSAV étrangers dont les contrôles de LBC-FT sont faibles ou inexistants en matière de dépôts liés aux rançongiciels. Les conclusions de la NMLRA ont éclairé la stratégie nationale américaine de lutte contre le terrorisme et les autres financements illicites de 2022, qui fournit des recommandations pour lutter contre les risques de financement illicite, ainsi que le plan d'action pour lutter contre les risques de financement illicite des actifs numériques.

Source : États-Unis

Coopération et coordination nationales

88. La recommandation 2 du GAFI exige que les États disposent de mécanismes nationaux permettant aux décideurs politiques, à la CRF, aux AEP et aux autres autorités compétentes de coopérer ainsi que de coordonner et d'échanger des renseignements. Les rançongiciels couvrent un large éventail de domaines, et les enquêtes peuvent impliquer des acteurs externes aux autorités traditionnelles de LBC-FT, comme les organismes de cybersécurité et de protection des données. Des mécanismes de coordination nationaux efficaces sont essentiels au regroupement de renseignements pertinents et différents experts, notamment du secteur privé, afin de fournir une réponse complète en matière d'atténuation de la menace posée par les rançongiciels et le blanchiment de capitaux connexe. Ces mécanismes permettent en outre l'échange critique de renseignements entre les autorités menant des enquêtes médicolégales préalables et des enquêtes parallèles sur le financement.

89. Parmi les pratiques exemplaires, citons la création d'équipes d'application de la loi ou d'organismes multidisciplinaires dédiés à la cybercriminalité (ou même uniquement aux rançongiciels). Ces organismes peuvent coordonner les enquêtes sur les rançongiciels et le blanchiment de capitaux connexe qui nécessitent un large éventail d'expertise (par exemple, des experts de la CRF ou de l' AEP, des procureurs, des ingénieurs techniques, des négociateurs, etc.). En

règle générale, cette approche implique des responsables de l'application de la loi ayant une expertise dans la localisation d'actifs virtuels et peut être un moyen utile de centraliser l'expertise technique en la matière, surtout lorsque les ressources ou les capacités sont limitées.

Encadré 22. Mécanismes de coordination pour centraliser les renseignements et l'expertise en matière d'enquête

Pour lutter contre cette cybermenace en constante évolution, le gouvernement américain a créé le National Cyber Investigative Joint Task Force (NCIJTF) en 2008. Le NCIJTF est composé de plus de 30 organismes partenaires des forces de l'ordre, de la communauté du renseignement et du ministère de la Défense, avec des représentants qui sont situés au même endroit et collaborent pour mener à bien la mission de l'organisme s'inscrivant dans une perspective pangouvernementale.

En tant qu'unique cybercentre regroupant divers organismes, il incombe principalement à la NCIJTF de coordonner, d'intégrer et d'échanger des renseignements pour soutenir les enquêtes sur les cybermenaces, d'effectuer et soutenir l'analyse des renseignements pour les décideurs communautaires et de contribuer aux autres efforts en cours dans la lutte contre la cybermenace nationale.

Vers la fin de 2014, le NCIJTF a créé la Virtual Currency Team (VCT) qui a concentré ses efforts sur la localisation des opérations de cryptomonnaie liées à la cybercriminalité. Cette équipe fournit un des services de localisation de cryptomonnaie à tous les membres du NCIJTF. Dans le cadre de leurs propres efforts d'enquête, les membres du NCIJTF tels que le Federal Bureau of Investigation (FBI) et les services secrets américains (USSS) ont créé leurs équipes individuelles pour localiser les actifs virtuels au fur et à mesure que leur utilisation augmentait lors de divers types de crimes.

Au début de 2022, le FBI a créé la Virtual Assets Unit (VAU), un centre principal pour les programmes de cryptomonnaie du FBI où les renseignements, la technologie et le soutien opérationnel seront acheminés vers d'autres divisions. Dans le VAU, des experts en actifs virtuels et des ressources interdivisions sont intégrés dans un groupe de travail pour intégrer, de manière transparente, les renseignements et les opérations dans l'ensemble du FBI.

Source : États-Unis

Coopération et accompagnement du secteur privé

90. Comme l'indique la section 5.2, l'interaction avec le secteur privé est utile pour atténuer certains des défis ciblés dans le présent rapport. Par exemple, les entités réglementées peuvent éprouver des difficultés à détecter et déterminer les opérations suspectes liées aux rançongiciels. Certains pays ont réussi à augmenter la fréquence et la qualité des déclarations de soupçons liées aux

rançongiciels en impliquant les entités déclarantes et en leur fournissant des conseils, comme des indicateurs d'alerte (consulter le document « Lutte contre le financement des rançongiciels : indicateurs de risques » de 2023 du GAFI) et des guides de détection.

Encadré 23. Guides australiens sur la criminalité financière

La Fintel Alliance[1] de l'Australie publie une gamme de ressources, comme des guides sur la criminalité financière, pour aider les entreprises à comprendre, à identifier et à signaler les activités financières suspectes, afin de détecter et de prévenir les activités criminelles.

Les guides sur la criminalité financière fournissent des renseignements détaillés sur les aspects financiers des différents types de crimes. Ils comprennent des études de cas et des indicateurs visant à aider le secteur des services financiers à identifier et détecter les opérations suspectes.

Pour aider à lutter contre les rançongiciels, l'AUSTRAC a publié, en avril 2022, des guides sur la criminalité financière axés sur l'abus criminel des monnaies numériques et sur la détection et l'interruption des rançongiciels. Ces deux guides fournissent des renseignements pratiques et des indicateurs de risque clés pour aider à détecter les attaques et à réagir lorsqu'une personne pourrait être la cible d'un rançongiciel ou tenter de tirer profit d'un paiement de rançongiciel. Les deux guides sur la criminalité financière sont disponibles sur le site Web d'AUSTRAC, en anglais seulement :

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

Source : Australie

1. Fintel Alliance est un partenariat public-privé australien regroupant des experts provenant d'un éventail d'organismes impliqués dans la lutte contre le blanchiment de capitaux, le financement du terrorisme et d'autres crimes graves. Parmi les partenaires de Fintel Alliance, on compte de grandes banques, des fournisseurs de services de transfert de fonds et des exploitants de jeux d'argent, ainsi que les forces de l'ordre et des organismes de sécurité d'Australie et internationaux.

91. Le type et le degré de collaboration avec le secteur privé pour lutter contre les rançongiciels varient selon les pays. Les partenariats public-privé (PPP) sont un modèle utile et compris de tous, bien qu'ils demeurent axés sur les intervenants traditionnels (plus précisément les banques et autres institutions financières, bien que les EPNFD soient de plus en plus impliquées) dans de nombreux pays. Leur composition exacte variera en fonction des buts et objectifs du PPP, mais des intervenants non traditionnels pourraient y participer. Dans le cadre d'une

prévention et d'une détection efficaces des rançongiciels, les PPP doivent être utilisés pour réunir les autorités chargées de l'application de la loi, les CERT locales, la CRF et les PSAV, en plus des entreprises de cybersécurité, des fournisseurs de télécommunications et des entreprises d'analyse de la chaîne de blocs (par exemple, à titre de sous-groupe ou de secteur opérationnel d'un PPP existant).

92. Les objectifs communs de ces PPP comprennent la sensibilisation des participants aux rançongiciels et au blanchiment de capitaux connexe, l'échange de renseignements sur les tendances actuelles et l'étude des menaces actuelles et émergentes. Ces mécanismes peuvent également favoriser de meilleures relations avec le secteur privé et peuvent encourager le signalement d'incidents.

93. De plus, les pays ont tiré parti des PPP pour atteindre divers objectifs d'application de la loi. Les PPP fournissent une plateforme utile pour communiquer des pistes tactiques, afin de générer des renseignements, permettre l'échange d'informationspour améliorer la détection des réseaux de mules et de blanchiment dans divers secteurs réglementés, et faire avancer les enquêtes.

94. Étant donné que les PSAV détiennent des renseignements essentiels à l'obtention de bons résultats en matière d'application de la loi (y compris la propriété de portefeuilles et les retraits en monnaies fiduciaires), l'établissement d'une coopération avec ce secteur peut également permettre aux autorités d'accéder rapidement aux renseignements pour la localisation d'actifs virtuels ainsi que la saisie et la confiscation efficaces des actifs.

Encadré 24. Projet GATEWAY et l'opération Cyclone d'INTERPOL

Ayant débuté en 2016, **le projet GATEWAY** est un cadre d'échange de données avec des entités privées pour échanger des renseignements relatifs à la cybercriminalité. Le projet renforce les partenariats entre les forces de l'ordre et l'industrie privée pour générer des données sur les menaces à partir de plusieurs sources et permettre à la police de prévenir les attaques. Les entités qui font partie du projet GATEWAY sont des acteurs pertinents dans l'écosystème de la cybercriminalité. Il s'agit notamment d'entreprises de cybersécurité, d'entreprises de renseignement sur les menaces, de PSAV et de banques.

Le cadre permet la fourniture et la réception de renseignements sur la cybercriminalité entre INTERPOL et le secteur privé, et il permet au secteur privé de prêter main-forte à INTERPOL lors de l'analyse de la cybercriminalité. Les partenaires du secteur privé sont impliqués, en raison de leur expertise technique, pour aider à déterminer le type d'infection de rançongiciels, s'il est inconnu, ainsi qu'à effectuer l'analyse de l'une des pistes d'attribution potentielles.

L'opération Cyclone[1] fait suite à des enquêtes policières mondiales sur des attaques contre des entreprises coréennes et des établissements universitaires américains par le groupe de menaces de rançongiciels, Cl0p. L'opération mondiale de juin 2021 a abouti à l'arrestation de six

membres de la célèbre famille des rançongiciels et a été coordonnée par INTERPOL, en collaboration avec les forces de l'ordre coréennes, ukrainiennes et américaines. Les suspects auraient facilité le transfert et l'encaissement d'actifs d'une valeur de plus de 500 millions de dollars au nom du groupe de rançongiciels. INTERPOL a déployé l'opération Cyclone à l'aide des renseignements fournis par ses partenaires privés dans le cadre du projet GATEWAY.

Source : INTERPOL

1. Pour de plus amples renseignements, veuillez consulter le lien suivant : https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2021/Une-operation-conduite-par-INTERPOL-aboutit-au-demantelement-d-un-reseau-tres-actif-de-cybermalfaiteurs

Mesures proposées

- Les gouvernements devraient veiller à cibler et à évaluer les risques de blanchiment des capitaux posés par les rançongiciels dans leurs évaluations nationales des risques. Compte tenu de la nature décentralisée des actifs virtuels et des groupes criminels de rançongiciels, cela comprend les États possédant des secteurs d'actifs virtuels pour lesquels les rançongiciels ne constituent pas, pour l'instant, une menace nationale. De telles constatations peuvent, en outre, contribuer à soutenir les cyberstratégies nationales en obtenant une vue d'ensemble nationale globale des risques liés aux rançongiciels.
- Les États devraient élaborer des mécanismes de coordination entre les autorités compétentes concernées, allant des autorités de poursuite pénale, de la LBC-FT et de la cybercriminalité, aux partenaires non traditionnels tels que les organismes de cybersécurité ou de protection des données. Cela favorise l'échange de renseignements et fournit une plateforme utile pour l'échange croisé de diverses expertises techniques.
- Les États devraient cibler et établir des mécanismes soutenant la coopération entre le secteur public et le secteur privé. Les États devraient envisager l'implication des PSAV et d'autres partenaires non traditionnels dans ces mécanismes de coopération.

Coopération internationale

95. Les attaques de rançongiciels et les flux financiers connexes sont souvent transnationaux et multinationaux. Les criminels utilisant un rançongiciel sont

généralement basés dans un pays différent des multiples pays par lesquels les fonds (notamment les actifs virtuels) sont blanchis et finalement « encaissés ». La complexité et les défis posés par les stratagèmes de blanchiment de capitaux liés aux rançongiciels nécessitent une coopération transfrontalière continue entre les autorités chargées de l'application de la loi disposant de renseignements, d'outils et d'une expertise pertinents. Il est impératif de mettre en place et d'exploiter les mécanismes actuels de coopération internationale pour mener à bien les enquêtes financières et le recouvrement des actifs, notamment lorsque des rançongiciels sont impliqués.

Encadré 25. Enquête internationale conjointe contre le rançongiciel Lockergoga

En janvier 2019, une grande entreprise française a été victime d'une attaque de rançongiciel. Le logiciel malveillant Lockergoga a été identifiée comme la source de rançongiciels utilisée pour chiffrer plusieurs fichiers et serveurs internes de l'entreprise. L'entreprise a refusé de payer la rançon de 410 bitcoins exigée à la suite de négociations. Cependant, Lockergoga a également été utilisé par des pirates lors de nombreuses autres attaques.

Eurojust et Europol ont formé une équipe commune d'enquête rassemblant plusieurs pays européens. Cela s'est traduit par un échange efficace de renseignements, ainsi qu'une coopération judiciaire au moyen de décisions d'enquête européennes (DEE) et du traité d'assistance judiciaire mutuelle, qui ont contribué à accélérer les enquêtes. Europol et Eurojust ont également fourni un soutien technique avec une grande capacité de matériel et de financement. Une infrastructure criminelle de commandement et contrôle a ensuite été identifiée; les flux de messagerie des pirates ont été décryptés, et le groupe a été finalement localisé dans un pays oriental. Par conséquent, plusieurs personnes ont été arrêtées dans ledit pays.

Des enquêtes sont en cours. Grâce à l'analyse de la chaîne de blocs, les enquêteurs ont dévoilé les différentes techniques de chaîne de pelage utilisées. L'un des principaux blanchisseurs de capitaux a été ainsi arrêté en Suisse. Plusieurs autres mules ont également été appréhendées dans différents pays. Les enquêtes ont en outre révélé que les rançons versées n'étaient pas destinées au seul profit du pirate informatique. Par exemple, des paiements illicites ont dû être versés à divers partenaires criminels et utilisés pour l'infrastructure (ingénieurs et développeurs de logiciels, hébergement à toute épreuve pour les serveurs sécurisés, services de RPV à toute épreuve pour masquer la communication ou la connexion aux serveurs de commande et contrôle, services de blanchiment de capitaux pour organiser les mouvements de la chaîne de pelage, etc.), ainsi que pour trouver des mules et des installations d'encaissement.

Source : France

96. Les renseignements recherchés dans les demandes internationales concernent généralement à la fois les preuves médicolégales requises pour les enquêtes préalables et les données financières nécessaires aux enquêtes sur le blanchiment de capitaux. Cela comprend les adresses IP situées à l'étranger, les noms et pseudonymes utilisés, les renseignements sur les abonnés, ainsi que les informations sur la propriété effective, les renseignements sur les opérations et ceux portant sur les contreparties relatives aux portefeuilles hébergés par des PSAV étrangers.

Défis spécifiques posés par l'utilisation des actifs virtuels

97. L'implication d'actifs virtuels dans le blanchiment lié aux rançongiciels peut créer de nouvelles difficultés dans la coopération transfrontalière. Les différences dans le traitement ou la réglementation des actifs virtuels dans les systèmes judiciaires, ainsi que l'implication ou la supervision limitée ou inexistante du gouvernement dans le secteur, dans certains pays, peuvent compliquer la capacité ou la volonté des autorités à participer à la coopération internationale.

98. Par exemple, les juridictions qui n'enregistrent pas ou ne supervisent pas les PSAV peuvent éprouver des difficultés à identifier les entreprises auprès desquelles demander des informations. Même si l'entité appropriée est localisée, les autorités peuvent alors n'avoir accès qu'à des techniques d'enquête contraignantes pour exécuter une demande de coopération internationale. Les renseignements pouvant être obtenus dans le cadre d'un processus de coopération informel peuvent, par conséquent, être limités.

99. Ce défi est exacerbé par le fait que de nombreux pays abritant des criminels utilisant des rançongiciels et leurs mules financières, ou encore les PSAV utilisés pour blanchir et encaisser les produits de ces criminels, tolèrent cette activité et peuvent être insensibles aux demandes d'application de la loi étrangère. Lorsque les PSAV se trouvent dans des pays sans obligations en matière de LBC-FT, ils peuvent tout simplement ne pas disposer des dossiers pertinents à mettre à la disposition des forces de l'ordre. Cette situation finit par contrecarrer les enquêtes financières en cours et les tentatives de recouvrement d'actifs. Ces défis renforcent de nouveau l'importance d'accélérer la mise en œuvre mondiale de la recommandation 15 du GAFI (notamment la règle d'acheminement).

Encadré 26. Difficultés d'enquête découlant de PSAV non coopératifs à l'étranger

L'entreprise X a été victime d'une attaque par ce que l'on croyait être le rançongiciel Caley. Après négociation, la victime a payé 0,25 bitcoin au criminel et a reçu la clé de déchiffrement par courriel. Les activités de la victime ont pu alors reprendre.

Les autorités ont été tardivement informées de l'affaire au moyen d'un rapport de police déposé par la victime plusieurs jours après avoir payé la rançon, ce qui a rendu la piste inutile. Selon l'analyse de la chaîne de blocs, la piste de paiement de la rançon a mené à un PSAV basé à

l'étranger, et il a été noté qu'un solde de 0,0081 bitcoin a été transféré vers un portefeuille virtuel hébergé par le PSAV étranger, qui est depuis resté réticent à coopérer malgré de multiples demandes de renseignements. Les enquêtes ont été davantage compliquées par l'utilisation d'un mélangeur pour brouiller les opérations. En raison des circonstances de l'affaire, l'auteur reste inconnu et aucune récupération d'actifs ou arrestation n'a pu être effectuée.

Source : Singapour

100. Les architectures réparties de certains PSAV (dont les opérations sont réparties dans plusieurs pays) peuvent également constituer un important fardeau d'enquête pour les forces de l'ordre lorsque celles-ci tentent de déterminer à quelle entité elles doivent demander des renseignements, ou bien vers quel pays se tourner pour demander du soutien. Par exemple, un pays a indiqué éprouver des difficultés à cibler le pays compétent auprès duquel demander de l'aide au sujet d'un IBAN qui appartiendrait, vraisemblablement, à un compte bancaire géré par un PSAV dans une institution financière étrangère. Un autre pays a souligné que certains PSAV semblent n'avoir aucune présence physique. Il devient alors difficile de savoir avec quel pays il faut coopérer.

Nécessité d'une coopération rapide

101. Étant donné que les criminels utilisant des rançongiciels peuvent se trouver n'importe où dans le monde et que les actifs virtuels peuvent être transférés presque instantanément, les forces de l'ordre doivent agir rapidement pour localiser les produits issus de rançongiciels et empêcher leur dispersion à l'étranger. Pour ce faire, des mécanismes officiels de coopération internationale (comme l'entraide judiciaire) sont généralement nécessaires pour obtenir des preuves et assurer les saisies dans le cadre d'une procédure pénale. Pourtant, ces mécanismes officiels de coopération ne sont pas toujours propices à la rapidité, ce qui peut considérablement ralentir, bloquer ou même contrecarrer les enquêtes. La complexité des enquêtes liées aux rançongiciels, en ce qui a trait au nombre d'entreprises et de pays impliqués, aggrave ces défis, car la coopération internationale prend plus de temps et de ressources pour les rançongiciels que pour d'autres activités criminelles.

102. Tirer parti de la coopération informelle peut être utile pour surmonter ces difficultés et peut contribuer à rationaliser et à accélérer les demandes d'entraide judiciaire. Certains pays ont souligné l'importance des communications actuelles pour faciliter la coopération en temps opportun. Ils ont donc établi des voies de communication informelles pour communiquer et interagir avec leurs contreparties étrangères. Cela permet de faciliter l'échange rapide de renseignements nécessaires pour faire avancer les procédures pénales, tout en respectant les processus nécessaires en place pour protéger ces renseignements. Un tel échange informel de renseignements peut se produire entre les CRF grâce à l'Egmont Secure Web, tandis que la coopération entre polices peut se produire au moyen du I-24/7 d'INTERPOL ainsi que d'autres réseaux informels, notamment le réseau CARIN et les réseaux ARIN. Les autorités devraient avoir mis en place des processus et des points de contact pour les

canaux de coopération internationaux et régionaux accessibles, afin de soutenir la localisation rapide des fonds et le recouvrement efficace des actifs.

103. Certains pays ont réussi à coopérer grâce à l'établissement de relations bilatérales. Recourir à des agents de liaison spécialisés dans la cybercriminalité situés à l'étranger peut faciliter considérablement l'échange de renseignements entre l'hôte de la liaison et le pays d'origine. Cela peut également permettre aux autorités de recueillir et de fournir des preuves depuis l'étranger dans le cadre d'enquêtes liées aux rançongiciels. Afin de promouvoir la coopération bilatérale, les autorités devraient envisager de rendre publics les processus et les points de contact pour la coopération, plus précisément pour faciliter la localisation rapide des fonds et le recouvrement des actifs.

Encadré 27. Projet CODA

Un cybercriminel canadien lié à des campagnes de rançongiciels et à la compromission informatique des ministères et des établissements médicaux de l'Alaska a été arrêté en novembre 2021 et accusé de multiples infractions liées à la cybercriminalité. Avant de contacter des partenaires internationaux, le FBI enquêtait sur plusieurs cyberintrusions criminelles connexes. Une fois le sujet identifié et localisé, le FBI a communiqué avec sa personne-ressource bilatérale au sein de la Police provinciale de l'Ontario (OPP).

Les deux pays ont alors entamé des enquêtes parallèles. Le Centre national de coordination en cybercriminalité (CNC3), Europol et les autorités hollandaises chargées de l'application de la loi ont offert leur soutien à l'OPP et au FBI. Le CNC3 a fourni un soutien opérationnel, des analyses de données et de comportement, des fiches et des rapports de renseignement, des services de localisation de cryptomonnaie et des analyses sur une période de 23 mois dans le cadre de l'enquête internationale. Ces efforts ont aidé à confirmer l'identification du sujet d'intérêt, menant à son arrestation ultérieure. L'utilisation de techniques analytiques de pointe et d'outils spécialisés, tels que la localisation de cryptomonnaie, est essentielle dans ces types d'enquêtes sur la cybercriminalité.

Source : Canada et États-Unis

Importance de la coordination multilatérale

104. Les études de cas présentant des mesures d'exécution fructueuses impliquent généralement des autorités compétentes de plusieurs pays. Cela correspond à la nature internationale et décentralisée des attaques de rançongiciels et du blanchiment de capitaux connexe. L'une des clés du succès est la nécessité d'une coordination internationale entre les pays concernés pour déraciner et interrompre simultanément les cyberconsortiums et leurs affiliés. Cette coordination atténue également la dispersion des risques où les organisations

criminelles peuvent facilement transférer leurs opérations numériques vers une autre zone protégée.

105. Plusieurs mécanismes internationaux de coordination des forces de l'ordre peuvent être utilisés à cette fin, par exemple Europol, Eurojust et INTERPOL. Ces derniers hébergent des bases de données et fournissent de la logistique et de l'expertise pour coordonner les intervenants de plusieurs pays. Ces mécanismes multilatéraux peuvent être utiles, surtout pour accélérer l'échange de renseignements critiques pour les enquêtes financières et le recouvrement d'actifs.

Encadré 28. Opération GoldDust[1]

En novembre 2021, les autorités roumaines ont arrêté deux individus soupçonnés de cyberattaques à l'aide du rançongiciel Sodinokibi/REvil. Ils seraient responsables de 5 000 infections et auraient empoché un total d'un demi-million d'euros grâce aux rançons. Depuis février 2021, les forces de l'ordre ont également arrêté trois autres entreprises affiliées à Sodinokibi/REvil et deux suspects liés à GandCrab. Ces arrestations font partie des résultats de l'opération GoldDust, qui a impliqué 17 pays[2], Europol, Eurojust et INTERPOL. Toutes les arrestations découlent des efforts conjoints des forces de l'ordre internationales d'identification, d'écoute téléphonique et de saisie de certaines des infrastructures utilisées par la famille de rançongiciels Sodinokibi/REvil, qui est considérée comme le successeur de GandCrab.

L'opération GoldDust a été mise sur pied à partir de pistes liées à des enquêtes antérieures sur GandCrab menées par la Roumanie avec le soutien d'Europol et des autorités d'application de la loi de plusieurs pays, dont le Royaume-Uni et les États-Unis.

Europol a facilité l'échange de renseignements, a soutenu la coordination de l'opération GoldDust et a fourni un soutien analytique opérationnel, en plus d'analyses médicolégales, de la cryptomonnaie et des logiciels malveillants. Europol a également envoyé des experts à chaque emplacement et mis sur pied un poste de commandement virtuel pour coordonner les activités sur le terrain. La coopération internationale a permis à Europol de rationaliser les efforts d'atténuation auprès des victimes avec d'autres pays de l'UE. Ces activités ont empêché les entreprises privées d'être victimes du rançongiciel Sodinokibi/REvil.

Le Joint Cybercrime Action Taskforce (J-CAT) d'Europol a soutenu l'opération. Cette équipe opérationnelle permanente est composée d'agents de liaison numériques de différents pays travaillant à partir du même bureau sur des enquêtes très médiatisées sur la cybercriminalité.

Source : Europol

Notes

1. Pour de plus amples renseignements, veuillez consulter le lien suivant [anglais seulement] : www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged
2. Pays participants : Australie, Belgique, Canada, France, Allemagne, Pays-Bas, Luxembourg, Norvège, Philippines, Pologne, Roumanie, Corée du Sud, Suède, Suisse, Koweït, Royaume-Uni, États-Unis.

Mesures proposées

- Les pays devraient établir des mécanismes bilatéraux, régionaux et multilatéraux, et y participer activement en utilisant, par exemple, des bureaux de liaison et en établissant des points de contact clairs et disponibles en tout temps, afin de faciliter une coopération internationale et un échange de renseignements rapides.

Conclusion

106. Malgré la récente croissance des flux financiers mondiaux liés aux rançongiciels, il existe toujours une absence notable d'enquêtes sur le blanchiment de capitaux connexe. Cette étude a montré que les rançongiciels sont un problème multidisciplinaire et international. Ils nécessitent une approche coordonnée, afin de répondre efficacement à la menace. Pour y parvenir, les pays devraient tirer parti des partenariats à trois niveaux : public-public, public-privé et avec d'autres pays et des organisations multilatérales.

107. Cette étude illustre l'importance d'une mise en œuvre accélérée des normes du GAFI pour fournir un cadre efficace de lutte contre les produits illicites dérivés des rançongiciels, plus précisément en ce qui concerne les actifs virtuels et les PSAV. Le GAFI continuera à promouvoir la mise en œuvre de ses normes dans ce secteur.

108. Pour conclure, le rôle des actifs virtuels dans le blanchiment des produits des rançongiciels et les techniques en constante évolution employées par les groupes criminels utilisant des rançongiciels présentent de nouveaux défis. Les autorités compétentes devraient veiller à ce que leurs lois demeurent pertinentes et soient dotées des compétences et des capacités requises pour faire preuve d'agilité dans un environnement criminel numérique dynamique.

www.fatf-gafi.org

Mars 2023

Lutte contre le financement des rançongiciels

Ce rapport du GAFI analyse les méthodes utilisées par les criminels pour réaliser leurs attaques par rançongiciels et la manière dont les paiements sont effectués et comment les recettes sont blanchies. Ils utilisent presque exclusivement des crypto-monnaies ou des actifs virtuels. Les criminels ont facilement accès à des fournisseurs de services d'actifs virtuels dans le monde entier. Le recours à des juridictions dont les contrôles LBC/FT sont faibles, voire inexistants est préoccupant.