GAFI

RAPPORT DU GAFI

Lutte contre le financement des rançongiciels

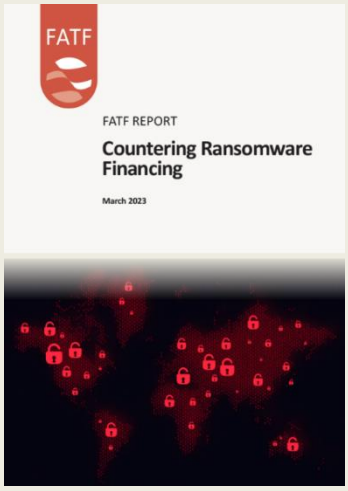
Indicateurs de risque potentiels

LUTTE CONTRE LE FINANCEMENT DES RANÇONGICIELS : INDICATEURS DE RISQUES

Les indicateurs de risque suivants s'appuient sur l'expérience et les données fournies par les pays du réseau mondial. Ces indicateurs visent à renforcer la détection des opérations suspectes liées aux rançongiciels. La liste est ensuite subdivisée en différentes perspectives tout au long du processus de paiement d'un rançongiciel.

Nous encourageons les lecteurs à consulter les notes ci-dessous à propos de la manipulation ainsi que le rapport du GAFI de 2023 sur la lutte contre le financement des rançongiciels avant d'utiliser les indicateurs de risques.

Lutte contre le financement des rançongiciels



Le présent rapport analyse les méthodes qu'utilisent les criminels pour mener à bien leurs attaques de rançongiciels et la manière dont ils blanchissent les paiements d'une rançon.

Le rapport souligne que les autorités doivent s'appuyer sur les mécanismes de coopération internationale actuels et en tirer parti pour lutter efficacement contre le blanchiment des paiements de rançongiciels. Elles doivent également obtenir les compétences et les outils nécessaires pour recueillir rapidement des renseignements clés, surveiller des opérations virtuelles quasi instantanées et récupérer des actifs virtuels avant qu'ils ne soient dilapidés.

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

L'existence d'un indicateur unique auprès d'un client ou lié à une opération ne peut, à elle seule, justifier des soupçons d'une infraction découlant d'un rançongiciel, et un indicateur unique ne fournira pas nécessairement une indication claire d'une telle activité. Cependant, cela pourrait entraîner une surveillance et un examen plus approfondis, le cas échéant.

La liste d'indicateurs complète la liste d'indicateurs d'alerte des actifs virtuels du GAFI [1] et s'applique aussi bien au secteur public qu'au secteur privé. En ce qui concerne ces derniers, les indicateurs peuvent être pertinents pour les PSAV, les banques et autres institutions financières et de paiement.

Banques et autres institutions financières et de paiement identifiant des paiements de la part de victimes de rançongiciels

- Des virements électroniques sortants vers des entreprises de consultation en matière de cybersécurité ou de réponse aux incidents spécialisées dans la résolution d'attaques de rançongiciels.
- Des virements électroniques entrants inhabituels provenant de compagnies d'assurance spécialisées dans la résolution d'attaques de rançongiciels.
- Un client signalant une attaque ou un paiement de rançongiciel.
- Des renseignements de source ouverte sur les attaques de rançongiciels visant leurs clients.
- Un volume élevé d'opérations du même compte bancaire vers plusieurs comptes d'un PSAV.
- Une description de paiement contenant des mots tels que « rançon » ou les noms des groupes de rançongiciels.
- Des paiements versés aux PSAV dans les pays à haut risque (consulter l'encadré).

PSAV identifiant des paiements de la part de victimes de rançongiciels

- Une demande d'achat d'actifs virtuels par une entreprise d'intervention en cas d'incident ou une compagnie d'assurance au nom d'un tiers.
- Un client déclarant au PSAV qu'il achète des actifs virtuels afin de payer une rançon.
- Un utilisateur sans aucun historique d'opérations concernant des actifs virtuels envoyant des fonds en dehors des pratiques commerciales courantes.
- Un client augmentant la limite d'un compte aux fins de virement à un tiers.
- Un client semblant anxieux ou impatient du temps de traitement d'un paiement.
- Des achats ou des virements impliquant des cryptomonnaies confidentielles.
- Des paiements versés aux PSAV dans des pays présentant un risque élevé.
- Un nouveau client achetant des actifs virtuels et transférant l'intégralité du solde de son compte vers une seule adresse.

[1] Consulter le rapport du GAFI, « Virtual Assets Red Flag Indicators of Money Laundering and Terrorism Financing » (septembre 2020), en anglais seulement : www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red- Drapeau-Indicateurs.pdf

PSAV identifiant la réception d'un paiement de rançongiciel ou le compte criminel lié au rançongiciel

- À la suite d'un premier transfert important d'actifs virtuels, un client ayant peu ou pas du tout d'activité liée aux monnaies numériques.
- L'analyse de la chaîne de blocs sur les adresses d'un portefeuille révélant des liens avec les rançongiciels.
- Un retrait immédiat après la conversion des fonds en actifs virtuels.
- Un envoi d'actifs virtuels vers des portefeuilles liés à des rançongiciels.
- Un recours à un PSAV dans un pays présentant un risque élevé.
- Un transfert d'actifs virtuels vers un service mélangeur.
- Un recours à un réseau crypté.
- Les renseignements de vérification sont une photographie de données sur un écran d'ordinateur ou ont un nom de fichier contenant « WhatsApp image » ou un nom similaire.
- La syntaxe du client ne correspond pas à sa démographie.
- Les renseignements du client montrent que ce dernier détient un compte de messagerie connu pour son niveau de confidentialité élevé, tels que Proton Mail ou Tutanota.
- Les données d'identification sont incohérentes ou une tentative de création d'un compte avec une fausse identité.
- Plusieurs comptes liés aux mêmes coordonnées; adresses partagées sous différents noms.
- Le client semble utiliser un RPV.
- Des opérations impliquant des cryptomonnaies confidentielles.

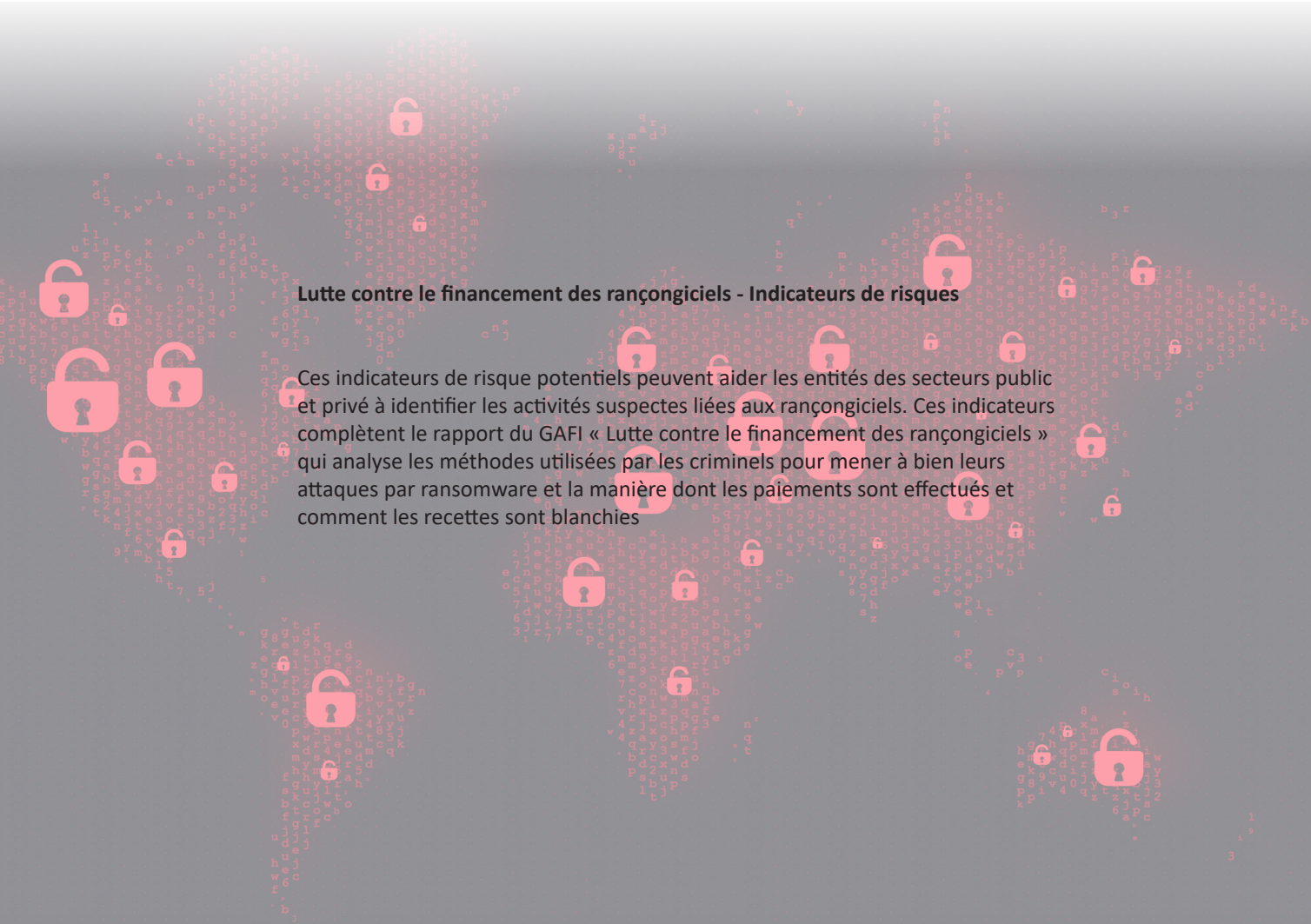
Encadré : États présentant des risques de blanchiment d'argent plus élevés

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 de risques de blanchiment d'argent ou de financement du terrorisme. 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.

www.fatf-gafi.org

Mars 2023



Lutte contre le financement des rançongiciels - Indicateurs de risques

Ces indicateurs de risque potentiels peuvent aider les entités des secteurs public et privé à identifier les activités suspectes liées aux rançongiciels. Ces indicateurs complètent le rapport du GAFI « Lutte contre le financement des rançongiciels » qui analyse les méthodes utilisées par les criminels pour mener à bien leurs attaques par ransomware et la manière dont les paiements sont effectués et comment les recettes sont blanchies