PARQUET GÉNÉRAL
DU GRAND-DUCHÉ DE LUXEMBOURG
CRF - Cellule de renseignement financier

Typologies COVID-19

Note

Version 1.0 du 02.04.2020

Ce document est destiné aux professionnels soumis à la loi modifiée du 12 novembre 2004 concernant la lutte contre le blanchiment et contre le financement du terrorisme.

Bureaux :
41B boulevard Franklin D. Roosevelt
L-2450 Luxembourg

Adresse postale :
L-2080 Luxembourg

Courriel : crf@justice.etat.lu
Internet : www.crf.lu
Téléphone : (+352) 47 59 81-447

INTRODUCTION

Les rapports publiés par Europol, Interpol et le GAFI montrent que des groupes criminels ont rapidement saisi l'occasion d'exploiter la crise liée au coronavirus et à la propagation de la maladie COVID-19, en adaptant leurs modes opératoires existants ou en se livrant à de nouvelles activités criminelles. La Cellule de Renseignement Financier (CRF) renvoie expressément vers la documentation publiée par ces entités :

- Europol : https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic
- Interpol : https://www.interpol.int/
- FATF / GAFI : https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html

La présente note a pour objectifs de :

a) Informer les professionnels soumis à la loi modifiée du 12 novembre 2004 concernant la lutte contre le blanchiment et contre le financement du terrorisme (ci-après : la Loi de 2004) sur l'existence de cette documentation ;
b) Sensibiliser les professionnels aux schémas y décrits ;
c) Partager un premier set d'indicateurs liés à des fraudes en lien avec le COVID-19,
d) Obtenir un retour d'information, afin de compléter cette liste d'indicateurs.

Le travail mené par la CRF est basé sur les analyses effectuées par les différentes organisations internationales et sur les déclarations d'opérations suspectes reçues au cours des dernières semaines. Notre analyse montre que la vigilance des professionnels soumis à la Loi de 2004 est essentielle pour la prévention et la lutte contre les types de criminalité rencontrés.

Pour aider les professionnels dans cette tâche, la présente note contient une liste d'indicateurs. Un indicateur, pris isolément, n'éveille pas forcément de soupçon. La présence de plusieurs des comportements repris ci-dessous devrait toutefois engendrer une vérification de la transaction.

Au regard des informations limitées à la disposition de la CRF, cette note aborde uniquement les indicateurs en matière de fraude. La CRF coopère avec ses partenaires internationaux pour améliorer et compléter la liste actuelle. Elle est naturellement à l'entière disposition des déclarants pour analyser d'autres sets d'indicateurs avec eux.

La présente analyse contient :

- Un aperçu des typologies constatées (1),
- Des précisions sur le processus de déclaration de soupçons en lien avec la crise du COVID-19 (2).

1 LES FRAUDES

Les fraudes analysées touchent majoritairement la vente de matériel utilisé pour lutter contre le coronavirus et contre la propagation de la maladie COVID-19. Les produits concernés sont notamment des masques de protection et des (prétendus) médicaments contre le virus et la maladie. Dans la suite de cette note, ces produits sont désignés comme « matériel COVID-19 ».

1.1 L'INGÉNIERIE SOCIALE

1.1.1 TYPOLOGIES RENCONTRÉES

Les fraudes visées sont notamment :

- La fraude au président,
- Le Business E-Mail compromise (BEC).

Plus d'informations sur ces fraudes sont reprises dans la note de la CRF sur les faux virements[1], ainsi que dans la documentation du groupe Egmont des CRF sur le business e-mail compromise[2].

Deux modes opératoires adaptés et développés autour de l'ingénierie sociale sont à distinguer :

- La crise du coronavirus est prise comme prétexte pour détourner des paiements,
- Des criminels se font passer pour des producteurs et distributeurs de matériel COVID-19.

La crise du coronavirus est prise comme prétexte pour détourner des paiements

Les fraudes au président et BEC sont désormais bien connues et de nombreuses campagnes de prévention ont été menées pour lutter contre ce phénomène[3]. Les criminels tirent profit de la situation créée par la crise, dont le confinement et les difficultés économiques, pour passer en dessous du radar de vigilance mis en place au sein des sociétés visées.

Voici deux exemples :

- Des criminels se font passer pour le dirigeant d'une société et contactent l'établissement financier de celle-ci. Le prétendu dirigeant explique que toute son entreprise est désorganisée et qu'il travaille à partir de son domicile. Il argumente qu'il ne saurait dès lors suivre les procédures usuelles (notamment de contresignature). Il va insister sur une communication qui passe exclusivement par e-mail.

- En tirant encore prétexte de la désorganisation d'une entreprise, des criminels argumentent que les paiements ne se font désormais plus sur les comptes centraux de la société, mais directement sur les comptes des sites de production. Ils peuvent notamment tirer argument de problèmes de trésorerie et de problèmes avec leur service comptable. Ce stratagème permet de détourner des paiements – effectués dans le cadre d'une relation d'affaires existante – sur des comptes frauduleux.

Du côté de la sécurité informatique[4], le travail à domicile crée de nouveaux risques. Des criminels peuvent exploiter ces failles pour gagner un accès à des documents confidentiels, utilisés par la suite dans le cadre de fraudes sophistiquées. Il faut rappeler que le vol d'informations privilégiées est une des raisons du succès des fraudes au président et BEC.

Des prétendus producteurs et distributeurs de matériel COVID-19.

En se servant de l'ingénierie sociale, des criminels se font passer pour des vendeurs de matériel COVID-19. La situation d'urgence constante dans laquelle des acteurs du secteur privé et public peuvent se trouver pour acquérir ce matériel crée une vulnérabilité accrue. Afin de donner crédit à leur offre, des criminels vont notamment :

- Produire de faux documents,
- Créer des sites Internet fictifs,
- Créer des sociétés écran,
- Se faire passer pour des entreprises sérieuses qui produisent effectivement le matériel en question.

[1] https://justice.public.lu/dam-assets/fr/legislation/circulaires/CRF-note-faux-virements.pdf
[2] https://justice.public.lu/dam-assets/fr/organisation-justice/crf/guidances/20190708-EGMONT-GROUP-BEC-BULLETIN-final.pdf
[3] Voir notamment : https://police.public.lu/fr/actualites/2018/10/w42/17-cyberscams.html
[4] Voir notamment : https://cybersecurite.public.lu

1.1.2 INDICATEURS RENCONTRÉS DU CÔTÉ DE LA VICTIME

1.1.2.1 « NOUVEAU » COMPTE BÉNÉFICIAIRE

Le client entretient des relations d'affaires avec un certain nombre de cocontractants. Soudainement, il entend effectuer un virement :

- En faveur d'un nouveau bénéficiaire et / ou
- En faveur d'un compte ouvert dans un pays dans lequel il n'exerce pas d'activité.

L'établissement financier doublera de vigilance lorsqu'un paiement effectué vers un nouveau bénéficiaire est rapidement suivi d'un nouvel ordre de transfert. En effet, les fraudeurs forts de leur premier succès ont tendance à procéder à un nouvel ordre de virement.

1.1.2.2 INCOHÉRENCES PAR RAPPORT À UN NOUVEAU BÉNÉFICIAIRE

Les incohérences suivantes peuvent notamment apparaitre en lien avec le bénéficiaire :

- Le bénéficiaire est une société écran,
- Le bénéficiaire est un nouvel acteur sur le marché et n'a pas d'expérience documentée dans le commerce de matériel COVID-19,
- Le bénéficiaire n'est pas le producteur du matériel, mais un tiers qui n'a pas de relation documentée avec le producteur,
- Le bénéficiaire n'a pas d'activité économique propre,
- Le compte bénéficiaire est situé dans une juridiction qui n'a pas de lien apparent avec la transaction à effectuer.

1.1.2.3 URGENCE DE LA TRANSACTION

Le client insiste sur l'urgence de la transaction à effectuer. Cette attitude peut faire suite à la pression exercée sur le client par le criminel, qui explique qu'en l'absence de paiement immédiat, sa marchandise – très convoitée – sera envoyée à un autre client.

1.1.2.4 NOMS DE DOMAINE FRAUDULEUX – PHISHING/PHARMING

Les instructions de virement proviennent d'un compte de messagerie ressemblant étroitement au compte de messagerie du client. L'adresse de messagerie a toutefois été légèrement modifiée en ajoutant, en modifiant ou en supprimant un ou plusieurs caractères.

> Exemples :
> contact@abc.com au lieu de contact@abc.lu
> contact@adc.com au lieu de contact@abc.com

Les instructions peuvent également provenir de la bonne adresse e-mail du client mais qui a été piratée. Ces cas de fraude sont plus sophistiqués.

1.1.2.5 INCOHÉRENCES DANS LA DOCUMENTATION

Les pièces justificatives remises au professionnel peuvent présenter des incohérences.

En premier lieu, les messages échangés entre le client et son prétendu cocontractant peuvent présenter des signes pointant vers du Phishing/Pharming (point 1.1.2.4 ci-dessus).

La documentation consultée par la CRF montre aussi que les criminels créent des sites Internet fictifs pour simuler une activité économique en lien avec la vente de matériel COVID-19. L'expérience de la CRF montre que les conditions générales de tels sites ne sont souvent pas cohérentes par rapport à la prétendue activité économique. Le niveau de détail des explications fournies sur des sites fictifs reste également très limité.

1.1.3 INDICATEURS RENCONTRÉS DU CÔTÉ DE L'AUTEUR (COMPTE BÉNÉFICIAIRE)

1.1.3.1 INCOHÉRENCE DU MONTANT DE LA TRANSACTION

Les montants perçus par le titulaire du compte bénéficiaire peuvent être incohérents par rapport au profil du client. Dans les affaires analysées par la CRF, des personnes ont ainsi reçu des montants de plusieurs dizaines de milliers d'euros, alors qu'elles ne bénéficiaient que d'un salaire modeste.

De tels comptes sont souvent ouverts par des « *money mules* », définis par Europol comme *« une personne qui transfère des fonds obtenus illégalement entre différents comptes bancaires ou autres, très souvent dans différents pays, pour le compte d'autrui. Les mules sont ainsi recrutées par les criminels pour recevoir de l'argent sur leur compte bancaire, afin de le retirer ou de le transférer sur des comptes détenus à l'étranger, souvent en contrepartie d'une commission »*[5].

1.1.3.2 INCOHÉRENCE PAR RAPPORT À L'ACTIVITÉ DU CLIENT

Le client a ouvert un compte pour recevoir des salaires d'un employeur local et reçoit des montants importants de l'étranger, sans lien avec l'exécution d'un contrat de travail.

Par exemple :

Le client est salarié chez une banque de la place et reçoit un virement de 25.000 EUR d'une entreprise française, avec comme objet du virement « Paiement de la facture 123456 ».

L'objet des ordres de virement perçus témoigne d'une incohérence par rapport à l'activité professionnelle du client, personne physique ou personne morale.

Par exemple :

Une société a été ouverte comme shelf company avec un objet social très général et perçoit soudainement des sommes d'argent en lien avec la vente de matériel COVID-19.

L'objet social de la société ne prévoit pas cette activité.

Par exemple :

La société a été ouverte sous la forme juridique d'une holding ou SOPARFI. Certains postes du bilan (chiffre d'affaires, salaires, cotisations sociales …) de la société ne sont pas en ligne avec les transactions projetées.

[5] https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling

1.2 LES FRAUDES S'ADRESSANT À UN PUBLIC PLUS LARGE

Les cas étudiés se rapportent à l'escroquerie et aux infractions à la propriété intellectuelle. Les schémas criminels sont classiques :

- Du matériel COVID-19 est mis en vente, mais jamais livré,
- Du matériel contrefait est vendu,
- La vente de médicaments en dehors des réseaux autorisés.

La commission de ces fraudes se fait essentiellement en ligne. A côté des places de marché qui peuvent être exploitées à cet effet, l'envoi de publicités par e-mail (SPAM) ou la publication d'annonces sur les réseaux sociaux est fréquente.

Pour plus de détails, il est renvoyé aux notes d'Europol, d'Interpol et du GAFI reprises ci-dessus.

1.2.1 LES INDICATEURS PAR RAPPORT AUX PRODUITS MIS EN VENTE

1.2.1.1 L'OBJET DE LA TRANSACTION

Les termes suivants peuvent notamment être utilisés dans l'objet de la transaction :

- COVID-19
- Coronavirus
- SARS-CoV-2
- Masque
- Mask
- FFP2
- FFP3
- "(personal) protective equipment" ou "PPE"
- Chloroquine
- Hydroxychloroquine
- Azithromycine
- Plaquenil
- Hand sanitizer
- Désinfectant
- Alcohol 70%
- Ethanol 70%
- Face shield
- Hazmat suits
- Decontamination suits
- Ventilator, respirator, or breathing machine
- Respiratoire artificiel
- Appareil respiratoire

1.2.1.2 LE PRIX DE L'OBJET

Des prix anormalement bas ou élevés par rapport à ceux pratiqués usuellement.

1.2.2 INDICATEURS PAR RAPPORT AU BÉNÉFICIAIRE DES TRANSACTIONS

- Le bénéficiaire est une société écran,
- Le bénéficiaire n'est pas actif dans la distribution de matériel COVID-19.

1.2.3 INDICATEURS PAR RAPPORT AU FONCTIONNEMENT DU COMPTE

La vente de matériel COVID-19 génère des entrées de fonds sur le compte, mais aucune dépense en lien avec cette activité n'est enregistrée sur le compte. Tel est notamment le cas si toutes les entrées de fonds sont utilisées à des fins privées par le titulaire du compte.

1.2.4 INDICATEURS PAR RAPPORT À LA VOIE DE DISTRIBUTION

1.2.4.1 VENTE DE PRODUITS EN DEHORS DES RÉSEAUX AUTORISÉS

p.ex. vente de médicaments à base de Chloroquine par Internet.

1.2.4.2 LIEN AVEC LE DARK WEB

Cet indicateur s'applique plus particulièrement aux prestataires de services d'actifs virtuels.

2 LE PROCESSUS DE DÉCLARATION

La CRF continue de recevoir et d'analyser les déclarations d'opérations suspectes conformément à sa note aux professionnels du 16 mars 2020 (Fonctionnement de la CRF – Covid-19)[6].

Les professionnels sont invités à signaler toute déclaration liée à la crise du coronavirus à la CRF. Ce signalement se fait en précédant la motivation de la déclaration du mot « COVID19 ».

[6] https://justice.public.lu/dam-assets/fr/organisation-justice/crf/info-covid19.pdf