
**FAQ – Questions posées lors du webinaire.**

Les délinquants financiers sont-ils plus armés (en termes de mode opératoire) que les enquêteurs ?

Ce n'est pas une question de plus ou moins armé. Les groupes criminels ont leurs propres outils et modes opératoires pour commettre leurs méfaits. Les enquêteurs ont les outils légaux pour identifier les criminels. La difficulté réside dans les actions de coopération internationale. Nous avons une compétence nationale et pour agir au-delà nous devons suivre les voies de la coopération judiciaire qui peut être plus ou moins longue, plus ou moins efficience (même avec l'aide d'Europol et d'Interpol).

L'ingénierie financière criminelle se base aujourd'hui principalement sur des cryptomonnaies (bitcoin, eth, ripple…) qui sont liées à des comptes non détectables par l'Etat, la montée de ces monnaies est un facteur motivateur des criminels pour s'agrandir.

Comment peut-on limiter les risques énormes liés à la non-détectabilité de ces monnaies ?

Certaines cryptomonnaies sont traçables (c'est le système de la blockchain), d'autres sont intraçables. Pour celles traçables, les criminels utilisent des mixeurs qui rendent le suivi des flux quasiment indétectable à un moment donné à la sortie du mixeur. La limitation des risques passera par la voie législative.

Est ce qu'il y a des secteurs d'activités touchés plus que d'autres ?

Non, les groupes criminels s'adaptent juste en fonction du chiffre d'affaires des entreprises et de l'information (ingénierie sociale) ayant pu être récupérée.

Et quel est le dimensionnement des entreprises les plus touchées ? Majors, ETI, TPE PME, Artisans

Aucun. C'est une question d'adaptabilité et d'opportunité des groupes criminels. Un escroc réalisera-t-il une attaque sur une entreprise mieux armée ou moins armée ? Vous avez la même réponse pour le cambrioleur : s'attaquera-t-il au pavillon avec alarme et système de surveillance ou à celui ne présentant aucune défense ?

L'étape décaissement/rencaissement via de l'argent liquide n'est-elle pas aujourd'hui en passe d'être remplacée par les cryptomonnaies ?

La difficulté restera toujours la problématique des espèces. Comment dois-je procéder pour transformer de la monnaie fiduciaire en monnaie scripturale ? Il s'agit de l'étape la plus difficile à réaliser en matière de blanchiment.

Cela ne permet-il pas d'accélérer l'étape "intraçable" et de s'abstraire du passage par une juridiction non coopérative, raccourcissant d'autant le temps disponible pour réagir ?

Si le paiement a lieu en cryptomonnaie, en effet. Mais il s'agit de groupes criminels qui réalisent des *ransomware* ou *ransomhack*. Je n'ai pas encore la connaissance d'entreprises qui règlent leurs fournisseurs en cryptomonnaie. C'est peut-être l'avenir !!! Une nouvelle fois, il faudra s'adapter tant les entreprises (en redoublant de vigilance et en accentuant la sensibilisation) que les forces de l'ordre (mais le blocage des fonds sera devenu impossible...).

Les chiffres donnés par le responsable du Sirasco sur les dernières années et jusqu'en 2020 (114 millions) concernent-ils seulement les faux virements où toute la criminalité financière y compris celle auprès de l'Etat (PGE, chômage partiel...) ?

Le chiffre de 114 millions d'euros ne concerne que les FOVI et exclu donc les détournements des aides de l'Etat.

Les fraudes à la TVA ou taxe carbone. En essor ?

Les fraudes à la TVA c'est possible mais je n'ai pas le recul sur le sujet. Les fraudes à la taxe carbone, non c'est du passé pour la France.

Où porter plainte en France ? j'ai observé qu'au commissariat de police, la réaction est lente. Rendez-vous tardif et ensuite personne n'a la courtoisie d'informer l'honnête citoyen sur les suites et le résultat.

Vous devez déposer plainte en commissariat ou gendarmerie, en fait le service territorialement compétent. Pour un fait commis, le rendez-vous ne doit pas être tardif, bien au contraire car la réactivité est importante. Pour les suites et le résultat de l'enquête, vous vous adressez par écrit au tribunal judiciaire qui vous répondra de la suite donnée à l'enquête.

Quelles sont vos attentes concernant le rôle des Banques dans le dispositif de lutte contre la fraude (Fovi, Ingénierie sociale, ...) ?

Les banques agissent de concert avec les services judiciaires sur le sujet. Elles créent des scénarii pour cribler les virements réalisés. Les banques ont une obligation de vigilance vis à vis de leurs clients.

A-t-on une idée du profil des criminels ? Ont-ils fait des études ? Comment arrivent-ils à être aussi efficaces dans leurs stratégies et connaissance du monde des entreprises ?

Ils ont une lecture attentive de la presse spécialisée. Ils obtiennent un certain nombre de renseignements par l'ingénierie sociale (internet, appel téléphonique en usurpant l'identité d'un tiers, *etc*.). Ils consultent le BOAMP (annonces des marchés publics et avis d'attribution) pour avoir une connaissance des marchés publics obtenus (dans le cas d'un FOVI au préjudice d'une administration ou un service public).

Une idée : pourquoi vos services ne montent pas des pièges à escrocs avec de faux profils alléchants de Financiers ou Comptables sur LinkedIn ou Facebook ?

Tant qu'aucune infraction n'est commise ou tentée, il sera difficile d'identifier un escroc, le contact qui peut être réalisé n'aura pas de suite.

La justice israélienne ne coopère donc pas du tout avec les pays victimes ?

Bien au contraire mais nous avons nos propres législations et systèmes juridiques.

Beaucoup de documents sociaux se trouvent dans les greffes des tribunaux de commerce pour une somme modique

En effet, voire d'une manière quasiment gratuite sur certains sites WEB.

Existe-t-il un dispositif d'accompagnement spécifique du Sirasco pour tester la faiblesse des entreprises ?

Non. Nous outrepasserions nos missions.

Il est indispensable de sensibiliser tous ses fournisseurs, les alerter de l'existence de ces comportements et de leur demander de vérifier toute commande "singulière" émanant du groupe en contactant leurs interlocuteurs habituels.

Tout à fait. Un escroc se fera passer pour l'un des clients du fournisseur pour obtenir de l'information de sa part puis ensuite se retournera vers le client en se faisant passer pour le fournisseur et lui demander un paiement de la ou des factures sur un nouveau compte bancaire.

La seule barrière est donc la formation de notre personnel. On a eu une 1ère tentative de vol, bloqué heureusement par chance, à la suite de la formation de sensibilisation, une deuxième tentative. Mais là blocage immédiat par les personnes en interne.

Oui tout à fait

Pouvons-nous signaler aussi des tentatives de fraude même échouées ?

Oui tout à fait à l'adresse mail sirasco-dcpj-financier@interieur.gouv.fr. **MAIS** à condition que la tentative contient une chaîne d'éléments, **au minimum** : mail, téléphone, IBAN fourni(s)