Dans la fabrique des nouvelles arnaques aux SMS

ENQUÊTE

En pleine explosion depuis deux ans, les fraudes de plus en plus sophistiquées associant textos, faux sites internet et appels directs font des ravages. «Libération», qui révèle une récente affaire visant un célèbre magistrat, a pu infiltrer des réseaux d'escrocs pour comprendre le phénomène.

Par **EMMANUEL FANSTEN** et **GURVAN KRISTANADJAJA**
Photos **MARTIN COLOMBET**

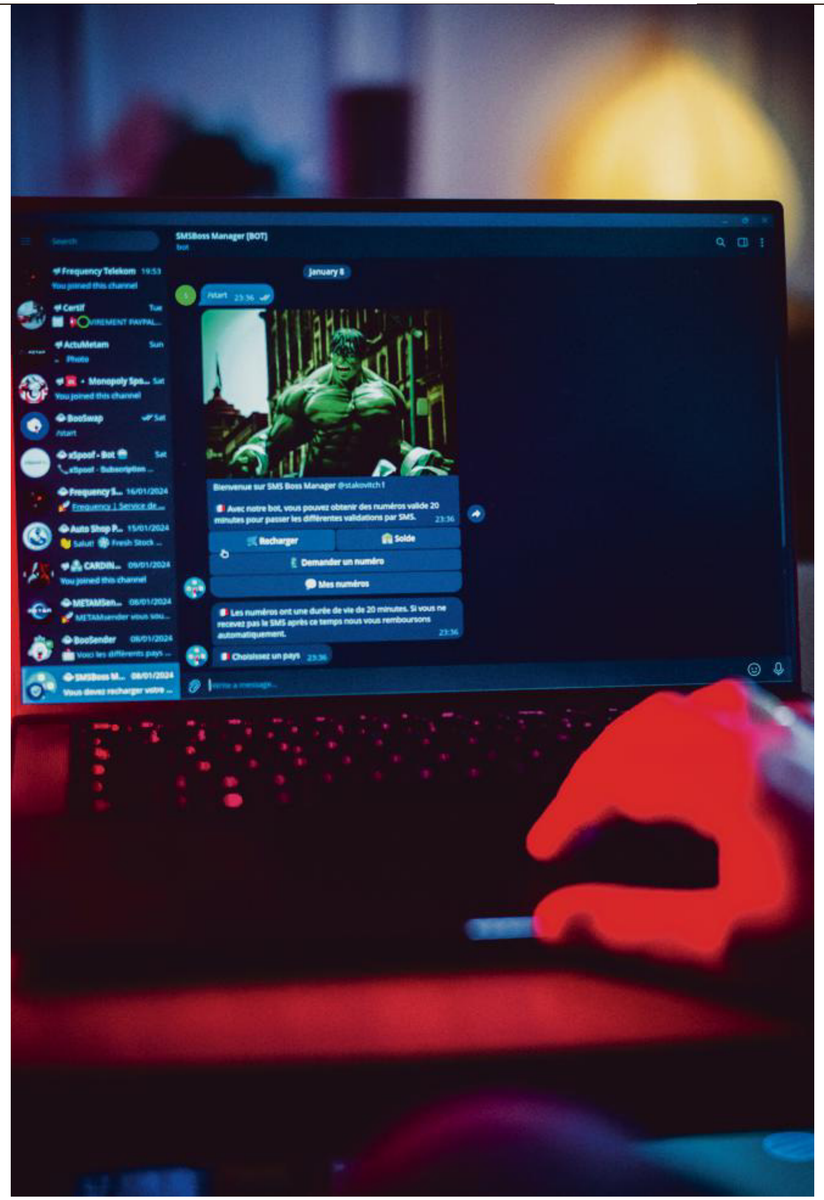
Fin septembre, l'ancien juge antiterroriste Jean-Louis Bruguière coule un dimanche paisible dans son appartement parisien avec son épouse, Catherine H., lorsque le téléphone de cette dernière retentit. L'homme au bout du fil se présente comme un employé du service anti-fraude de la BNP où le couple est client de longue date, et lui explique qu'un virement suspect de 2500 euros vers le Sénégal vient d'être détecté. Prudente, Catherine H., par ailleurs avocate au barreau de Paris, demande des garanties à son interlocuteur, qui l'invite alors à vérifier sur Internet que le numéro avec lequel il l'appelle est bien celui de sa banque. En quelques clics, la voilà rassurée. Ce détail n'est pas le seul à la mettre en confiance. Son correspondant dispose également de nombreuses informations confidentielles sur ses données bancaires et celles de son mari : l'ensemble de leurs avoirs, la nature de leurs comptes, les montants qui y figurent ou le nom des bénéficiaires de leurs virements. Une mine de renseignements que seule la banque est censée détenir. Au fil de la discussion, entrecoupée de pauses musicales typiques des services clients durant lesquelles le conseiller simule des vérifications, Catherine H. est invitée à faire opposition sur de prétendus nouveaux achats frauduleux. Mais alors qu'elle pense les annuler en communiquant un code, elle ne fait que les valider. A chaque étape, l'avocate reçoit un texto de «BNP PARIBAS» confirmant la pseudo-opération.

Découper les cartes en deux

Sous prétexte de mieux comprendre la fraude qu'il est lui-même en train de commettre, le faux conseiller bancaire va alors demander à sa cible de remettre à ses services sa carte bleue et celle de son mari à des fins d'analyse. Pour faciliter cette démarche, il indique que la banque est partenaire de la société G7 et qu'un taxi va l'attendre en bas de chez elle. Et pour la rassurer un peu plus, il lui demande de découper les cartes en deux, puis de les glisser dans une enveloppe numérotée. Quelques minutes plus tard, Catherine H. s'exécute et descend remettre sa carte au chauffeur qui patiente déjà au pied de son immeuble. Deux heures après, toujours en ligne au côté de son mari, elle redescend confier à un deuxième taxi la carte de ce dernier. Loin de se rendre au service anti-fraude de la banque, les chauffeurs vont en fait remettre les cartes à deux jeunes filles, qui s'empressent de multiplier les achats dans des boutiques de luxe sur les Champs-Elysées et d'effectuer des retraits en liquide au distributeur.

Mais l'escroquerie ne s'arrête pas là. Toujours au bout du fil, l'homme explique désormais que le couple semble être la cible d'un puissant réseau de cybercriminels basé à Dubaï. Un gang dangereux qui ne se contenterait pas de pirater les comptes de ses victimes, mais irait jusqu'à les cambrioler. D'où l'impérieuse nécessité pour eux, poursuit le faux conseiller, de sécuriser au plus vite leurs biens de valeur. Face au scepticisme de l'avocate et de son mari, l'homme explique ne pas avoir accès à l'enquête judiciaire sur ce réseau, mais transfère aussitôt l'appel à un second interlocuteur, qui se présente comme *«brigadier-chef à la Brigade de fraude au moyen de paiement»*, le service spécialisé de la PJ parisienne. Le faux policier complice leur confirme que les voyous sont susceptibles d'agir dans les heures ou les jours qui viennent. Après plusieurs heures de conversation quasi ininterrompue, Catherine H. consent à remettre à un troisième taxi un sac de voyage à l'intérieur duquel elle a glissé ses bijoux les plus précieux, des pièces d'or ●●● et même 30 000 euros en liquide qui dormaient dans l'appartement. En à peine une demi-journée, le couple a été délesté d'environ 200 000 euros.

Le lendemain, lorsqu'ils comprennent avoir été dupés, Catherine H. se rend au premier district de police judiciaire pour porter plainte. L'affaire prend alors un tour cocasse. Lors de son audition, le faux conseiller bancaire la rappelle sans savoir qu'il est désormais enregistré par les policiers. Toujours aussi sûr de lui, l'homme demande à l'avocate si elle a réfléchi à la sécurisation de sa maroquinerie et de ses œuvres d'art. En entendant le faux conseiller bancaire, les policiers reconnaîtront formellement un suspect bien connu de leur service, Emmanuel B., interpellé fin 2021 et incarcéré durant seize mois pour avoir escroqué des dizaines de victimes, dont l'ancien ministre de l'Economie Dominique Strauss-Kahn, détroussé de 25 000 euros l'été précédent après avoir benoîtement communiqué au téléphone ses codes bancaires, utilisés pour acheter des bijoux Cartier à Madrid. Dans une écoute judiciaire réalisée à l'époque, on l'entendait se targuer de gagner fréquemment 200 000 euros par semaine. Interpellé de nouveau mi-décembre 2023, Emmanuel B. a démenti être l'auteur des coups de fil à la femme du juge Bruguière, soulignant que le mode opératoire n'était pas le même que pour DSK. Une défense acrobatique qui ne l'a pas empêché d'être mis en examen pour *«escroquerie en bande organisée»* et *«association de malfaiteurs»*. Au total, dans ce dossier, 25 personnes ont été touchées, pour un préjudice de plus de 600 000 euros.



Thomas Damonneville, expert en sécurité, fondateur de la plateforme Stalkphish, piste les communautés de «scammers».

Montres de luxe, liasses de billets…

Cette affaire, que révèle *Libération*, illustre l'explosion des escroqueries téléphoniques plus ou moins sophistiquées, une tendance lourde depuis un an qui touche de plus en plus de victimes avec des préjudices très variables… Pour comprendre la recrudescence de ces pratiques, quelques recherches simples sur les réseaux sociaux et les messageries téléphoniques cryptées suffisent. Sur Snapchat, Discord, Telegram et de manière plus anecdotique Instagram, des jeunes Français forment une communauté de *«scammers»* – de l'anglais *«scam»*, qui signifie *«escroquerie»*. Ils s'échangent quotidiennement des conseils pour rendre leurs arnaques les plus crédibles possible. Sur un groupe Telegram réunissant plus de 10 000 membres, on se fait passer pour un jeune homme intéressé par une de ces fraudes. *«Tu peux aller jusqu'à 10k* [10 000 euros, ndlr] *à la semaine si t'es chaud bro»*, se vante un de ces escrocs. *«Ça va te changer la vie, c'est un conseil, tu fais 1,5 k-2 k par semaine sans forcer, quasiment tous les jours,* nous détaille un autre. *Si tu travailles, tu peux faire ça le soir, mais c'est mieux la journée pour* call [appeler en anglais, ndlr] *les victimes. Après tu peux faire des paiements sur des sites.»*

Pour preuve de ce qu'ils avancent, on découvre sur les réseaux sociaux des vidéos d'hommes arborant des montres de luxe, des liasses de billets, des factures d'achat de 3 500 euros dans une boutique Dior ou des bouteilles de champagne achetées en boîte de nuit. On perçoit chez ces jeunes, peu avares en conseils, un sentiment de complicité et d'entraide qui entretient l'esprit de groupe. Ils ont un langage à part, fait de mots courts issus de l'anglais, et gèrent leur activité comme Suite page 18

«Il faut s'adapter à des groupes plus imaginatifs»

Pour faire face à une cybercriminalité croissante depuis 2020, la justice s'est dotée d'outils législatifs et de services de police spécialisés, explique la vice-procureure Johanna Brousse.

Cheffe de la section en charge de la cybercriminalité au sein de la Juridiction nationale de lutte contre la criminalité organisée (Junalco) du parquet de Paris, la vice-procureure Johanna Brousse, 38 ans, alerte sur la sophistication croissante des escroqueries téléphoniques.

Comment ce type de délinquance a-t-il évolué ces dernières années ?

C'est un phénomène en hausse constante. Au-delà des dossiers parisiens liés à notre ressort géographique, nous avons aussi une compétence nationale pour les affaires les plus complexes et celles qui nécessitent une centralisation en raison d'un nombre de plaintes important. A ce titre, en 2023, nous avons traité 655 dossiers d'atteinte à un système de traitement automatisé de données, soit une augmentation de 7 % par rapport à l'année précédente. Pour ce type d'infractions, le véritable tournant a eu lieu en 2020, année au cours de laquelle nous avons constaté une hausse de 529 %. Cette explosion est due à la fois au confinement lors du Covid et à une transformation numérique en profondeur de la société. Les criminels ont compris qu'eux aussi avaient besoin du numérique, et on a constaté un basculement de la délinquance traditionnelle vers la cybercriminalité, tout aussi lucrative mais moins risqué en termes d'identification et de risques pénaux encourus.

Quel est le profil de ces criminels ?

Pour ce qui est du «smishing» *[hameçonnage par SMS, ndlr]*, il n'y a pas de profil type. Cela va des attaques assez peu structurées à des choses beaucoup plus complexes. Mais globalement, on observe une sophistication croissante des moyens utilisés. On est passé d'un mode opératoire assez artisanal à des méthodes plus rodées, avec par exemple l'utilisation d'Imsi-catchers (matériel d'espionnage théoriquement réservé aux services de renseignement) ou le recours à des sociétés spécialisées dans la vente en gros de données personnelles servant à mettre en place les escroqueries. Il existe désormais tout un écosystème destiné à faciliter ce type d'infraction, dans lequel évolue une criminalité très organisée avec des groupes parfaitement aguerris, dont certains viennent de l'est de l'Europe pour commettre ces faits sur notre territoire. On note aussi la recrudescence d'escroqueries menées en France depuis des centres d'appel en Tunisie, au Maroc, à l'île Maurice ou à Chypre. Il peut y avoir chez certains jeunes une sorte d'addiction à cela. Dans un dossier récent, le rapport d'expertise psychiatrique d'un suspect mentionne qu'il était «cyberaddict».

Comment faire face à des réseaux aussi structurés ?

Il est nécessaire de s'adapter à des groupes toujours plus imaginatifs et dangereux. Au sein de la section cybercriminalité de la Junalco, nous sommes passés de trois à cinq magistrats, avec des profils très techniques. Notre dernière recrue est un normalien agrégé de mathématiques spécialisé en intelligence artificielle. Cela marque une volonté forte de renforcer nos effectifs et de s'adapter à la transformation numérique de la délinquance, mais cela reste insuffisant. Nous pouvons également nous appuyer sur deux assistants spécialisés et une juriste dévolue à l'entraide pénale internationale. Ce travail en équipe est essentiel, on est très loin de l'entre-soi et du travail solitaire parfois décrit dans la magistrature.

Lors de notre enquête, nous avons également identifié de nombreux groupes d'escrocs échangeant des informations sur Telegram en toute impunité…

C'est un de mes combats. On en a déjà démantelé beaucoup, et on est en train d'investir encore davantage ce champ. De nouveaux outils législatifs nous permettent depuis un an de lancer de plus en plus d'investigations de ce type, en particulier sur Telegram ou Discord. Grâce aux services de police spécialisés, nous avons aussi la possibilité de mener des surveillances, de lancer des enquêtes sous pseudonyme et de faire des coups d'achat *[technique spéciale qui permet de piéger un escroc en se faisant passer pour un client ou un acheteur potentiel, ndlr]* afin de vérifier la réalité de ce qui est proposé à la vente. Cela permet de matérialiser l'infraction et de pouvoir renvoyer ces groupes devant le tribunal. Enfin, nous avons la possibilité de hacker directement des plateformes criminelles, notamment sur le darknet. Cela nous permet d'identifier les administrateurs, mais aussi de récupérer les données et de les rediriger vers les parquets concernés. Il n'y a plus, comme ça a pu être le cas auparavant, de zone d'impunité.

Recueilli par **E.Fn.** *et* **G.K.**
Photo **LAURA STEVENS**


Johanna Brousse, au tribunal de Paris, vendredi.

Suite de la page 17 une véritable petite entreprise. Ils vendent des formations à l'escroquerie pour 300 euros, des cartes bancaires volées pour 50 euros ou encore des «packs id» comprenant un lot de cartes d'identité, relevés d'imposition, taxe foncière et bulletins de salaire d'une victime pour 80 euros. Tout le matériel nécessaire pour devenir un parfait «scammer». Et pour prouver leur bonne foi, ils vont jusqu'à relayer des avis de clients satisfaits de leurs services, comme on le ferait sur un site marchand légal.

Selon l'un des référents du groupe Telegram, toutes les arnaques commencent par du hameçonnage, une pratique destinée à leurrer l'internaute pour l'inciter à communiquer ses données personnelles. Ils mettent donc en ligne des sites internet imitant des formulaires de l'assurance maladie, de la Poste ou de Netflix par exemple. Bien souvent, ils s'adaptent à l'actualité : pour Noël, ils vont privilégier les arnaques Colissimo, à la rentrée de septembre celles au crédit conso. Ils ont recours à des services d'hébergement simplifié pour la mise en ligne – qui permettent notamment de générer plusieurs URL sur une seule adresse IP. Tout est disponible en kit pour quelques dizaines d'euros. *«Il faudra choisir un nom de domaine puis l'acheter. Dans cet exemple, je prendrai netflix-secure.com. […] Pour les SMS, pas besoin de développer, vous pouvez utiliser un message simple comme "Netflix : Vos informations de paiement ont expiré. Merci de les mettre à jour via le lien suivant"»,* explique notre initiateur.

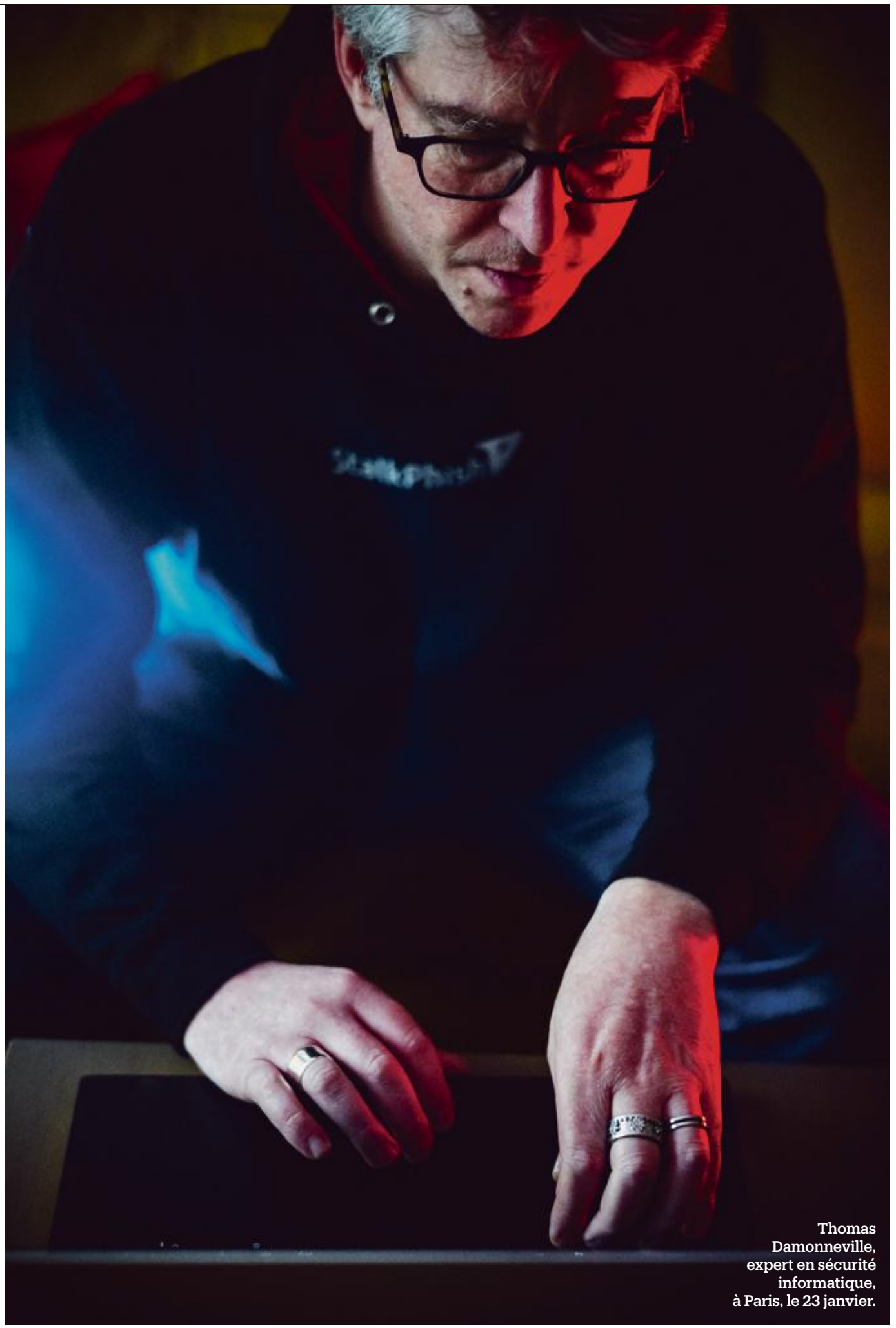
Libération a aussi identifié des dizaines de faux noms de domaine à consonance familière, comme ali-exprex.fr (au lieu d'Ali Express), yahoot.fr (à la place de Yahoo). Il s'agit ensuite d'acquérir une liste de plusieurs milliers de numéros de téléphone issue de fuites de données ou de précédents hameçonnages que l'on trouve, là encore, pour moins de 30 euros sur Telegram ou sur Discord. Pour envoyer les messages, les escrocs ont recours aux services d'applications permettant de détenir un ou plusieurs numéros sur un seul téléphone comme OnOff. L'appât est en place, il ne reste plus qu'à attendre que ça morde. Quand une personne se fait avoir, ils reçoivent simplement ses informations via les faux sites.

«L'intonation et le vocabulaire»

C'est à ce moment que l'arnaque débute réellement. Munis des données personnelles glanées – souvent des numéros de carte de crédit, des copies de carte d'identité ou de passeport, des RIB ou même des copies de l'acte de naissance – ils contactent leurs victimes, en se faisant passer le plus souvent pour un conseiller bancaire – comme ce fut le cas dans l'affaire visant le juge antiterroriste Bruguière ou DSK. Pour gagner leur confiance, ils divulguent des détails de leur identité grâce aux documents récupérés lors du hameçonnage et ont recours au *«spoofing»,* une pratique consistant à modifier l'intitulé associé au numéro entrant grâce à un logiciel afin d'afficher (et d'usurper) celui de la banque.

Au sein des groupes Telegram, certains surnommés les *«alloteurs»,* se sont fait une spécialité de ces coups de téléphone. Ils sont capables de reprendre les codes et les langages des services des fraudes des banques à la perfection et prennent une commission sur le butin. *«Dispo allo now»,* écrivent-ils à toute heure de la journée sur les communautés en ligne pour vendre leurs services. Dans une enquête judiciaire ouverte pour des faits d'escroquerie en bande organisée, que *Libération* a pu consulter, l'un de ces *«alloteurs»* explique qu'il est nécessaire de bien manier *«l'intonation et le vocabulaire»* pour être crédible. *«On appelait les victimes pour valider un paiement, elles croyaient faire quelque chose de bien»,* détaille-t-il. D'autres procédures sur des fraudes plus poussées, dont *Libération* a pris connaissance, confirment aussi cette répartition systématique des tâches : l'échange avec les victimes est confié à une personne qui sait correctement parler, sans accent particulier, avec la patience suffisante, connaissant parfaitement le fonctionnement des interfaces bancaires, notamment les liens d'achat, les délais de notification, les plafonds de virement…

Lorsqu'elles sont en confiance, certaines victimes transmettent leurs identifiants bancaires aux escrocs en quelques minutes à peine, permettant à ces derniers de réaliser des virements ou des achats en ligne. Certains arnaqueurs vont plus loin et commandent des taxis à l'adresse de leurs cibles pour récupérer leurs moyens de paiement, et proposent de couper leur carte bleue en deux pour la rendre prétendument inutilisable, comme ce fut le



Thomas Damonneville, expert en sécurité informatique, à Paris, le 23 janvier.

> «N'importe qui peut monter une arnaque. Ces gens-là proposent des hébergements déjà prêts à quatre ou cinq euros.»
>
> **Thomas Damonneville**
> expert en sécurité

cas pour le juge Bruguière. Une fois réceptionnée, ils n'ont en réalité qu'à la recoller pour réaliser des achats.

Le sentiment d'impunité des escrocs est frappant au sein de ces communautés. On y parle librement et on s'y vante comme si ce qui avait lieu anonymement sur Internet n'était pas répréhensible pénalement. Lorsqu'on a proposé à l'un d'eux de témoigner sur son activité illicite dans nos colonnes, il nous a traités de *«condé* [policier]*»*, avant de poursuivre sa vie au sein du groupe Telegram comme si de rien n'était. *«Ils veulent faire de l'argent facile et ils s'amusent. Ils ont l'impression qu'utiliser une messagerie cryptée empêche de les tracer. Sauf qu'en fait ils laissent des traces partout»*, assure Thomas Damonneville, expert en sécurité, fondateur de la plateforme Stalkphish et observateur discret de ces communautés.

Il y a deux ans, le quadragénaire a décidé de récupérer le code source des faux sites utilisés dans ces arnaques pour remonter jusqu'à leurs propriétaires et mieux analyser le phénomène. Sur son ordinateur, il suit régulièrement leurs faits et gestes. Evolution marquante depuis quelques mois selon l'expert, il n'est plus nécessaire d'avoir des compétences poussées en informatique pour faire du hameçonnage. *«Pour dix euros, n'importe qui peut aujourd'hui monter une arnaque. Ces gens-là proposent des hébergements déjà tout prêts à quatre ou cinq euros, par exemple.»* Ce qui explique que le nombre de victimes explose, de tout âge et de tous les milieux sociaux.

Un «phénomène massif»

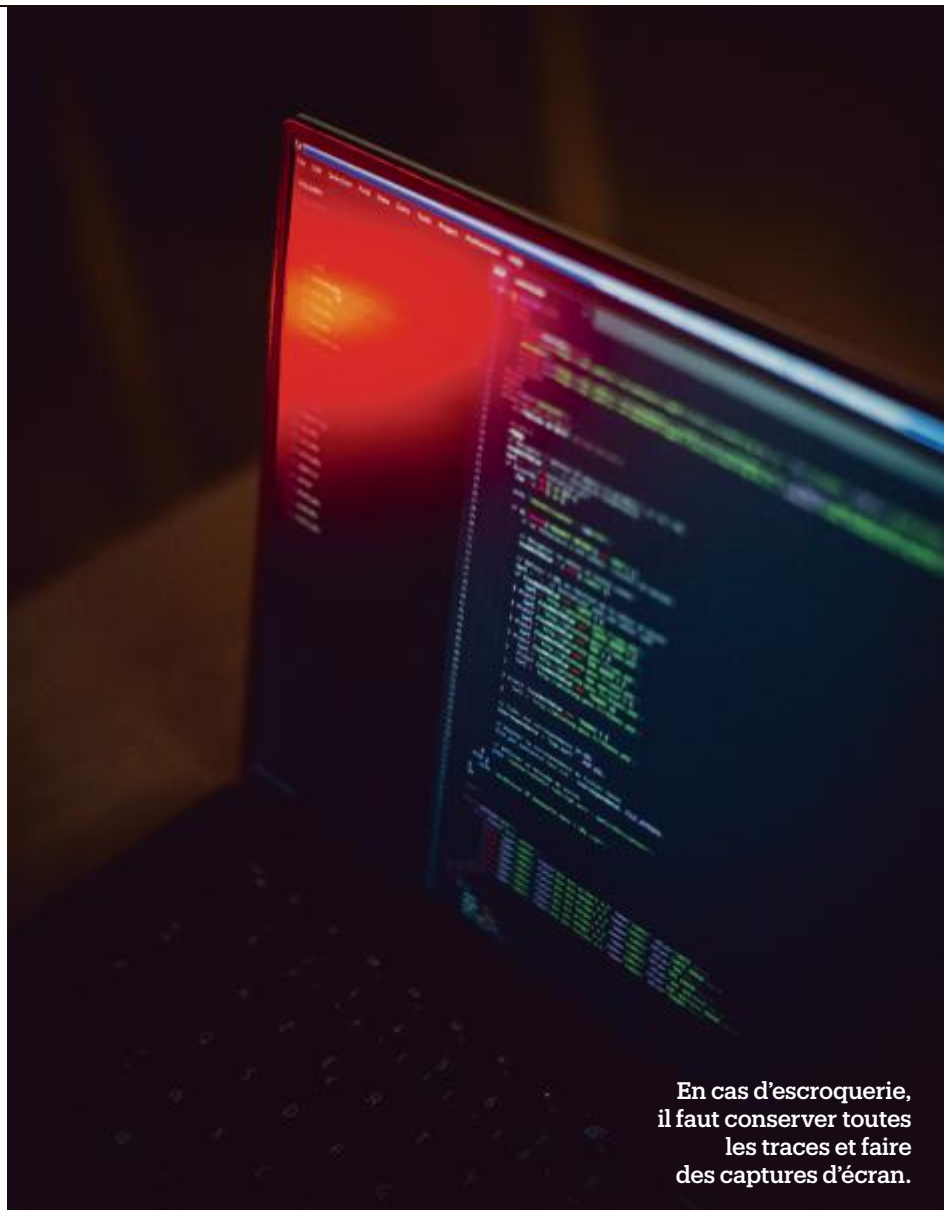
Dans les procédures consultées par *Libération*, la plupart de ces petits fraudeurs n'ont pas de casier judiciaire ou sont seulement connus pour des faits mineurs liés à l'usage ou au trafic de stupéfiants. Ils agissent souvent seuls dans leur chambre ou entourés de quelques femmes *«alloteuses»*, ils sont jeunes, parfois mineurs. Certains y ont vu une opportunité de gagner de l'argent facilement, après un parcours scolaire chaotique comme A., 30 ans, qui dit avoir *«enchaîné les petits boulots»*. Ils affirment lors de leurs interrogatoires avoir été galvanisés par l'effet de groupe et la simplicité d'accès aux informations en ligne.

Directeur général du site Cybermalveillance.gouv.fr, plateforme d'assistance aux victimes créée en 2017, Jérôme Notin constate un *«phénomène massif»* depuis environ trois ans, d'autant plus difficile à endiguer qu'il évolue constamment. Impossible toutefois de le quantifier avec précision. *«Entre les victimes réelles, les demandes d'assistance et les plaintes, il existe une importante déperdition»*, explique le spécialiste, qui parle même d'un *«chiffre noir»* des victimes. Pour dresser la typologie de ces escroqueries, la plateforme s'appuie notamment sur un réseau de 1200 prestataires de proximité susceptibles de fournir une assistance aux personnes visées, qui constituent autant de *«capteurs»* permettant de remonter des éléments techniques sur les modes opératoires utilisés. Jérôme Notin décrit un *«spectre très large»*, des arnaqueurs à la petite semaine aux groupes criminels très organisés, capables de jongler d'une escroquerie à l'autre.

Un constat partagé par Johanna Brousse, cheffe de la section cybercriminalité au sein de la Juridiction nationale de lutte contre la criminalité organisée, qui met en garde de son côté contre la mainmise de groupes de plus en plus structurés *(lire ci-contre)*: *«On a vu un certain nombre de mineurs commencer par de petites choses et poursuivre ce genre de pratiques avec des infractions de très haute volée.»* De nouvelles formes d'arnaques qui s'ajoutent à d'autres, en vogue ces dernières années.

Six personnes viennent ainsi d'être jugées à Paris pour des escroqueries réalisées lors du confinement du printemps 2020. Les aigrefins passaient des centaines d'appels par jour à des hôpitaux, des cliniques et des pharmacies pour leur vendre des masques et du gel hydroalcoolique qui n'arrivaient jamais à destination. Tous opéraient depuis un appartement transformé en *call center* en Israël. L'argent était ensuite blanchi via une multitude de comptes bancaires à l'étranger. Dénonçant le caractère *«abject»* des faits, le parquet a requis jusqu'à cinq ans de prison contre le cerveau présumé de l'affaire, un homme déjà condamné pour escroquerie et blanchiment. Dans ce dossier, le jugement doit être rendu le 7 février.

Au sein des communautés en ligne en perpétuelle ébullition, d'autres arnaques émergent chaque semaine tant les escrocs tentent de s'adapter en permanence aux réponses mises en place par les banques et par l'Etat. Ces derniers temps, des maires de communes rurales de l'Aveyron, du Morbihan, de la Meuse ou de Charente ont alerté sur l'apparition de nouvelles tentatives de hameçonnage très ciblées et géolocalisées. Dans des SMS, les fraudeurs se faisaient passer pour la municipalité et incitaient à remplir un dossier pour l'installation prochaine de panneaux solaires. Cette fois, les messages étaient adressés à des populations âgées, isolées et moins informées. ◆◆



En cas d'escroquerie, il faut conserver toutes les traces et faire des captures d'écran.

Dix règles pour éviter les arnaques

Face aux tentatives de hameçonnage par SMS, il faut être vigilant sur l'identité de l'émetteur du message et ne pas dévoiler d'informations personnelles. «Libé» vous donne ses conseils.

Ces dernières années, le nombre de SMS frauduleux a explosé. Leurs émetteurs se font passer pour des services de la Poste, des impôts, de Netflix ou encore de la police mais ils sont en réalité des usurpateurs qui tentent de vous arnaquer. Pour éviter les pièges, il est important de respecter des règles strictes.

1 Vérifiez l'émetteur et le contenu du message. Quand vous recevez ce type de message, il peut être difficile de savoir s'il est frauduleux ou non. Commencez par regarder le numéro d'envoi. S'il est inconnu, soyez vigilants. De même, s'il y a une faute d'orthographe dans le message, c'est probablement une tentative de hameçonnage.

2 Ne cliquez jamais sur le lien. Souvent, les URL (adresses web) transmis par les fraudeurs tentent de reproduire le nom de domaine du service qu'ils usurpent (lapostes.fr au lieu de laposte.fr par exemple). Dans le doute, préférez passer directement par le site émetteur. Ainsi, si vous recevez un message de Colissimo qui exige que vous payiez des frais de douane, connectez-vous directement à votre compte sur le site de Colissimo pour vérifier si c'est bien le cas.

3 Ne téléchargez jamais d'application en dehors des boutiques officielles. Vous n'avez pas respecté la règle numéro 2. Un site vous propose de télécharger une application. Déclinez, préférez passer directement par l'App Store ou Google Play. De même, si l'on vous demande de transmettre votre carte d'identité, votre RIB ou vos relevés d'imposition, méfiez-vous.

4 Ne communiquez jamais vos identifiants bancaires. Personne d'autre que vous ne doit pouvoir avoir accès à votre espace bancaire. Si votre banquier vous demande de vous transmettre vos codes, c'est qu'il n'en est pas un.

5 Utilisez un mot de passe complexe et différent à chaque fois. Pour votre adresse mail, vos comptes sur les réseaux sociaux, pour payer vos impôts… Dès lors que vous devez créer un compte en ligne, utilisez un mot de passe complexe (au moins une majuscule et un caractère spécial) et différent. Exemple: Gégédu33_2016-Netflix pour sécuriser votre compte Netflix et Gégédu33_2016-Ameli pour celui de l'assurance maladie.

6 Signalez chaque message suspect. Il existe un numéro simple auquel il est possible de transférer chaque message frauduleux: le 33 700. Plus il y a de signalements, plus la lutte contre la fraude est efficace car cela permet aux services concernés d'identifier d'éventuelles nouvelles escroqueries. Pour avoir des conseils, contactez la plateforme Info Escroqueries de la police au 0 805 805 817.

7 Raccrochez et rappelez. Si un conseiller bancaire tente de vous joindre un soir ou un week-end, soyez méfiants. En cas de doute, raccrochez, rendez-vous sur un moteur de recherche pour trouver le numéro de votre banque. Appelez leurs services pour vérifier que vous n'êtes pas victimes d'une tentative d'arnaque.

8 Gardez toutes les preuves. Malgré tous ces conseils, vous vous rendez compte que vous êtes victime d'une escroquerie. Dans ce cas, conservez toutes les traces et faites des captures d'écran.

9 Changez vos mots de passe et faites opposition. Il est important d'entraver l'activité des fraudeurs. Pour ce faire, modifiez vos mots de passe, remplacez-les par des combinaisons complexes (voir règle numéro 5) et si vous décelez des opérations suspectes sur vos comptes en banque, faites opposition.

10 Portez plainte. Rendez-vous dans un commissariat de police ou une brigade de gendarmerie proche de chez vous muni des preuves en votre possession. Vous pouvez être accompagné gratuitement par l'association France Victimes au 116 006 (appel et service gratuits), numéro d'aide aux victimes du ministère de la Justice. Service ouvert 7 jours sur 7 de 9 heures à 19 heures. Vous trouverez des informations sur le site cybermalveillance.gouv.fr.

E.Fn. *et* **G.K.**