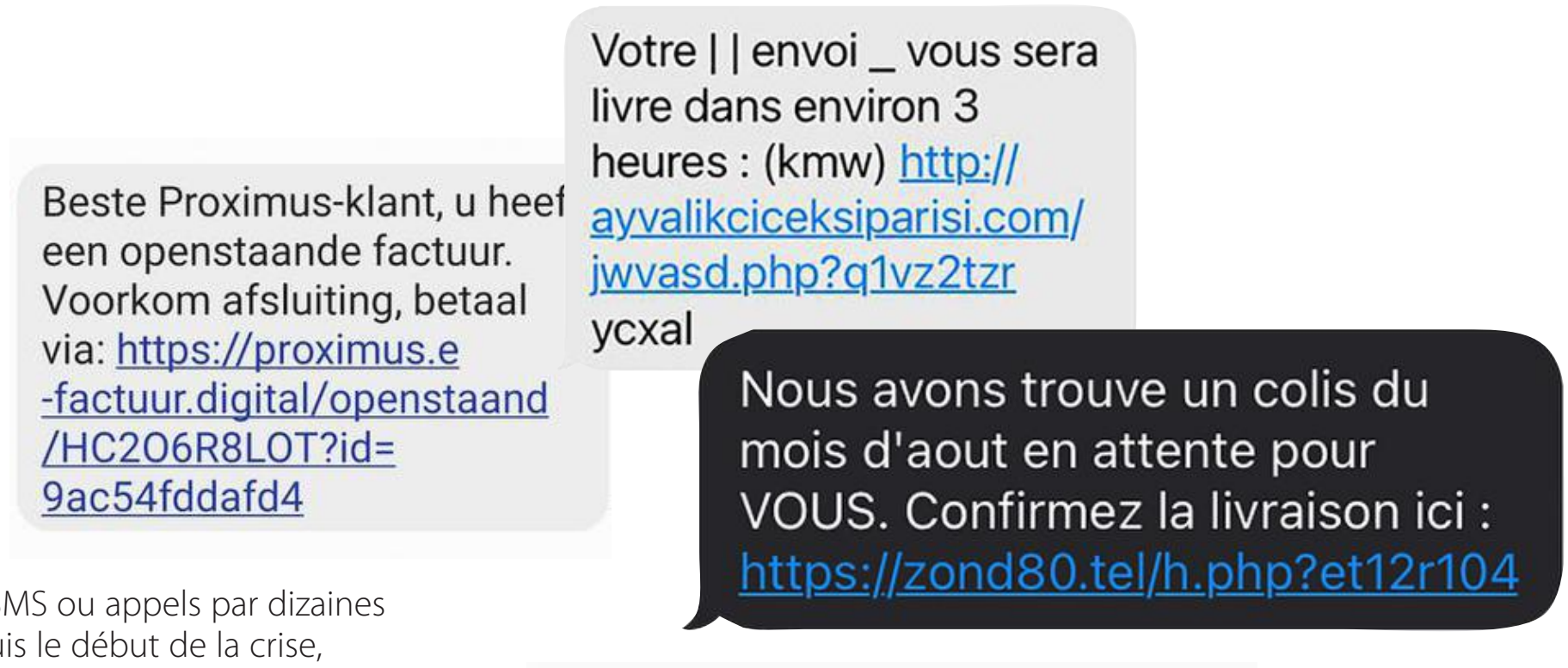
LA SEMAINE DE L'INFO CONSTRUCTIVE #SICBE21

ESCROQUERIE

Le journalisme constructif enrichit les pratiques journalistiques en proposant une vision plus nuancée de la société, en abordant les perspectives et les solutions et en portant une attention particulière aux mots et aux illustrations utilisés dans le traitement de l'information.
A l'occasion de la Semaine de l'info constructive, Le Soir mettra l'accent sur ces aspects à travers des dossiers, portraits et reportages indiquant comment ces pratiques sont rentrées dans notre quotidien.

Phishing, smishing… l'autre épidémie qui a envahi notre quotidien



Des faux mails, SMS ou appels par dizaines de milliers. Depuis le début de la crise, le phishing, ou hameçonnage, a pris une ampleur inédite. Son objectif : soutirer des données bancaires ou faire ouvrir insidieusement à une victime son portefeuille. Des attaques de plus en plus sophistiquées, menées par des cyberescrocs peu inquiétés.

CÉCILE DANJOU

Un SMS de bpost indiquant des frais à régler pour un colis, un mail du SPF Finances vous demandant de mettre à jour vos données bancaires, un appel du numéro de Card Stop vous demandant de choisir un nouveau code secret… L'illusion est de plus en plus subtile et n'épargne plus personne. L'hameçonnage, plus couramment appelé phishing – contraction des mots anglais *fishing* (pêche) et *phreaking* (piratage téléphonique) –, ne cesse de prendre de l'ampleur chez nous. Tout comme ses déclinaisons : le smishing, très en vogue dernièrement, qui désigne une arnaque via SMS, et le vishing, une fraude vocale. Partout, les chiffres explosent.

Premier arrêt au Centre pour la cybersécurité en Belgique (CCB). Son adresse suspect@safeonweb.be, qui permet à un particulier de signaler une fraude, a été prise d'assaut l'année passée, avec la réception de 3,2 millions de messages d'internautes. C'est quasi deux fois plus qu'en 2019, et cela représente près de 9.000 signalements par jour. Un chiffre déjà dépassé puisqu'actuellement, environ 12.000 mails sont traités quotidiennement. Le SPF Economie a, lui, reçu 30 % de signalements en plus via son point de contact en 2020. La statistique reprend toutes les fraudes, mais celles liées à internet arrivent en pole position.

Facilité et anonymat

Détour par les commissariats, où les dépôts de plaintes ont plus que triplé entre 2019 et 2020. Une évolution impressionnante, qui n'illustrerait que la partie émergée de l'iceberg. « Encore beaucoup de gens n'osent pas porter plainte car ils ont honte de s'être fait avoir », constate Olivier Bogaert, commissaire à la Computer crime unit de la police fédérale. Reste un dernier chiffre, livré par Febelfin, l'association du secteur bancaire : 34 millions d'euros ont été dérobés en 2020 via 67.000 transactions frauduleuses. Des arnaques de quelques centaines d'euros, la plupart du temps, mais qui dépassent parfois les 40.000 euros.

Le phénomène était déjà en marche avant la crise, mais son évolution a pris une direction exponentielle au fil des différents confinements. Peu étonnant : tout le monde s'est alors retrouvé à la maison, plus que jamais connecté. Les commandes et paiements en ligne ont explosé, tout comme le nombre de données cédées ici et là. De quoi créer un boulevard gigantesque pour les escrocs, parsemé de peu d'obstacles : pas de risque d'être surpris comme lors d'une effraction, pas de trace d'ADN, facilité de l'usurpation d'identité en ligne, anonymat quasi garanti… On parle même de « reconversion » de bandes organisées déjà existantes. « Certains criminels actifs dans le trafic de stupéfiants ont trouvé des avantages dans le numérique : on est à distance, on est plus discret », confirme Olivier Bogaert. Et puis il y a ces jeunes, débrouillards en informatique, qui ont besoin d'un peu d'argent.

« On assiste à une dématérialisation de la délinquance de rue », observe-t-on également au parquet de Bruxelles. Une criminalité qui se perfectionne. L'époque du mail bourré de fautes d'orthographe d'un mystérieux prince nigérian paraît bien lointaine. « Aujourd'hui, les imitations sont très bien faites. Et les messages sont adaptés à l'actualité. Pendant la crise, c'étaient de fausses notifications de bpost ou du SPF Santé publique. Bientôt, ce seront les offres exceptionnelles en électricité et en gaz », prédit Olivier Bogaert.

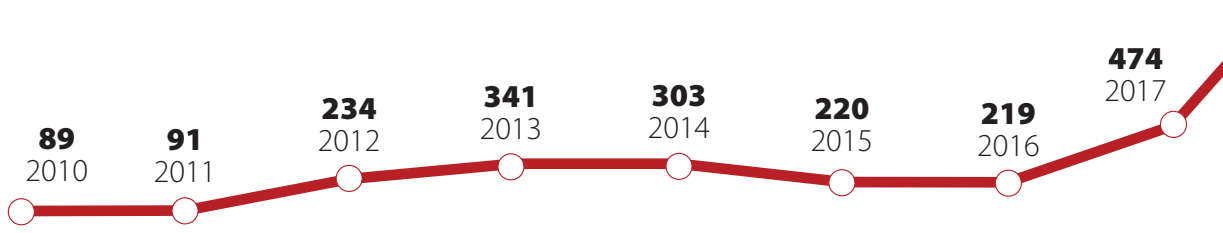
Pour bien comprendre le succès du phishing, il faut se plonger dans le *modus operandi* des pirates des temps modernes. Première surprise, pas besoin de chercher bien loin pour dénicher certains outils utilisés. Sur Google, on trouve des logiciels ou applications de spoofing, qui permettent de déguiser un numéro par un autre, fiable et connu. Exemple : vous recevez un appel, le numéro de votre banque ou de Card Stop s'affiche. Grâce au spoofing, c'est en réalité un hameçonneur qui est derrière. L'arme est évidemment redoutable.

100 euros la liste de 10.000 mails

Toujours sur Google, on trouve également des listes à vendre, venant de fuites de Facebook ou LinkedIn, par exemple, et contenant des numéros de téléphone, parfois de comptes bancaires, des mails, des adresses, des mots de passe, etc. Dans un long reportage d'investigation sur le sujet, des journalistes de la VRT montrent comment ils ont pu se procurer une liste de 10.000 adresses mails pour à peine 100 euros, ou encore les données complètes (bancaires comprises) d'un quadragénaire bruxellois pour… 35 euros. Mais pour Giannino Cuignet, hacker « éthique » à la tête de la start-up Redsystem, enseignant à l'Eurometropolitan e-Campus de Tournai ainsi qu'à la Sorbonne, à Paris, acquérir des données est une chose, les utiliser pour voler de l'argent en est une autre. C'est ici que l'on arrive à l'étape de l'inébranlable anonymisation. « Si le hameçonneur ne s'anonymise pas correctement, il va se faire repérer tout de suite. Or, cette opération est complexe. Souvent, il va coupler plusieurs techniques. Il va utiliser les services d'un VPN russe, payable en bitcoins, par exemple. Puis passer par plusieurs adresses IP dans le monde. Si les autorités investiguent, elles vont tomber sur la dernière adresse IP, mais de là, il leur sera quasiment impossible de remonter. »

L'anonymisation concerne aussi le transfert de l'argent. Pour celle-ci, les cybercriminels n'hésitent pas à recourir à des mules. Ce sont des personnes – souvent des jeunes ou des individus qui ont des besoins financiers – qui acceptent, pour une somme d'argent, de prêter leur compte bancaire pour des transits d'argent. Une autre option est l'utilisation des bitcoins. « Il y a des techniques, comme les "mixeurs", pour brouiller les traces et les transferts en bitcoins deviennent très difficiles à suivre », poursuit Giannino Cuignet.

Complexité pour remonter jusqu'aux criminels, pour suivre les mouvements financiers… Justice comme police acquiescent. Plutôt deux fois qu'une. « On remonte les données techniques pour essayer de remonter plus haut, mais c'est très très complexe, car les escrocs peuvent être dans d'autres pays, passer par des plateformes intermédiaires, il y a des entités asiatiques qui sont actives là-dedans… », décrit Olivier Bogaert. « Le plus souvent, on arrive à attraper les mules. Mais on est conscient que ce ne sont pas les vrais criminels », souligne Fleur Collienne, substitut du procureur du Roi à Liège et magistrate référente en criminalité informatique. « C'est une matière où on trouve beaucoup de dossiers classés sans suite, avec auteur inconnu. Malheureusement, on se sent un peu impuissant. » Même sentiment dans la capitale. « Certaines enquêtes aboutissent et mènent à des condamnations de mules bancaires, voire de recruteurs ou de personnes placées plus haut dans les organisations. Mais la justice doit faire face à de nombreux obstacles : le caractère transnational de ce type de fraudes, ce qui rend l'exercice de pour-



Nombre de plaintes (PV) enregistrées par les services de police locaux et fédéraux

Captures d'écran de tentatives d'escroquerie. © D.R.