La bonne fortune des cyberdélinquants

En 2018, près de 68 000 infractions numériques ont été enregistrées par la gendarmerie

La délinquance numérique continue de prendre de l'ampleur. En 2018, 67 890 infractions numéques ont été enregistrées selon s chiffres – forcément partiels – e la gendarmerie, qui dispose e statistiques plus fines que police en matière de dépôts e plainte. Soit 7 % de plus qu'en)17. Au-delà des piratages médiaques et techniquement très évoés, la majorité des faits est, en alité, souvent d'un piètre niau technique et ne débouche ıe sur des préjudices individuels bles. Mais leur caractère massif généralisé coûte cher, note le)port annuel sur les cybermeces du ministère de l'intérieur, ılisé par la délégation ministélle aux industries de sécurité et ı lutte contre les cybermenaces misc), publié mardi 9 juillet.

a grande majorité des actes lveillants numériques relèvent *« escroqueries liées à Internet »* : :s rassemblent plus de 73 % des ractions qui ont fait l'objet d'un)ôt de plainte dans une gendarrie. Le ministère de l'intérieur me que le préjudice total des roqueries en ligne s'élève à plus milliard d'euros en 2018.

aques aux cryptomonnaies

mi celles visant les particus, qui ont fait florès en 2018, fie l'arnaque au faux support

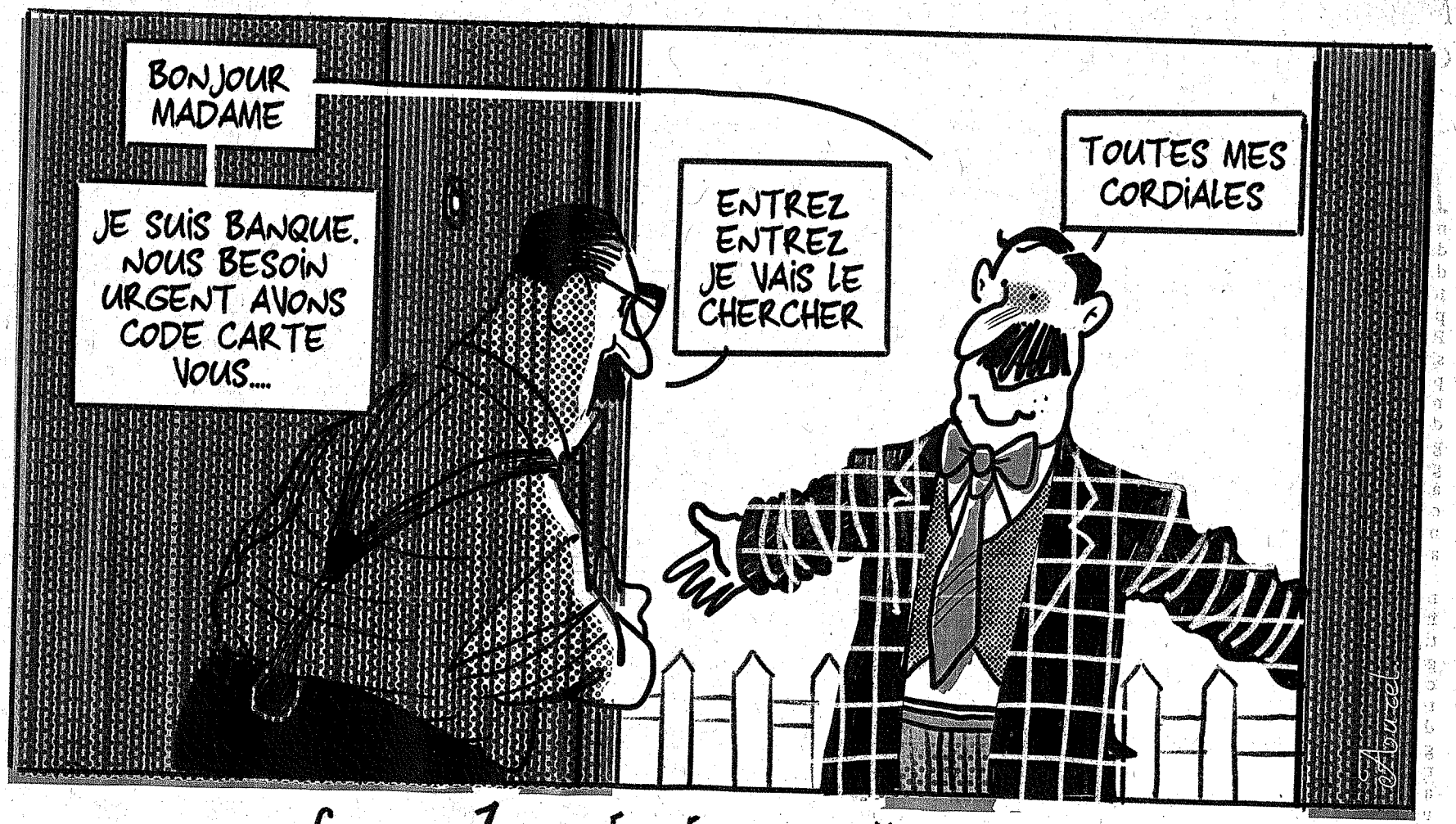

fig 1. Le phishing "à l'ancienne"

nsables convainquent des in-
nautes alpagués sur des sites
rencontres de leur transfé-
d'importantes sommes d'ar-
nt – a aussi fait de nombreuses
times. L'unité spécialisée en
ercriminalité de la police na-
nale a arrêté, en avril 2018, six
lividus s'adonnant à cette pra-
ue. Le groupe démantelé a ex-
qué plus de 3 millions d'euros.
es sites de « Forex », où les in-
nautes parient sur la hausse ou
baisse de diverses monnaies,
nt aussi partie des principales
roqueries recensées par les
torités. Les internautes pensent
oir affaire à une plate-forme lé-
ime avant que ses responsables
paraissent dans la nature, ren-
nt impossible la récupération
leur gain et même de leur mise
départ. Le montant du préju-
e s'élèverait à plusieurs centai-
s de millions d'euros.
es arnaques aux cryptomon-
ies se sont aussi développées
rande vitesse, suivant un

mis en examen, dont trois ont été écroués pour escroquerie en bande organisée : ils organisaient de faux investissements en cryptomonnaies et auraient détourné 5 millions d'euros.

Les fraudes à la carte bancaire – piratage par Internet ou captation du numéro de carte sur les distributeurs par exemple – sont aussi très importantes. Ainsi, la plate-forme Perceval, mise en place en juin 2018 et qui permet à tout un chacun de signaler facile-

Des actes malveillants qui ont fait l'objet d'un dépôt de plainte, 73 % relèvent des escroqueries liées à Internet »

depuis novembre environ 450 alertes par jour, pour un montant moyen de 480 euros. Depuis la mise en ligne de ce site, le montant des signalements dépasse les 55 millions d'euros.

Les entreprises sont aussi lourdement touchées. Ces derniers mois, l'évolution des « rançongiciels », ces virus qui bloquent l'accès aux données avant de demander une rançon pour les déverrouiller, inquiète les autorités. A des vagues de contamination massives succèdent des opérations d'infection plus ciblées, et donc plus coûteuses.

« Les attaques par rançongiciel semblent davantage cibler les grandes entreprises ayant la capacité de payer des rançons très élevées », écrivent les auteurs du rapport. Plusieurs groupes français en ont dernièrement fait les frais : Altran, société spécialisée dans l'ingénierie, le géant de l'agroalimentaire Fleury Michon ou, plus récemment, Eurofins, tou-

Après des années de sensibilisation, les escroqueries aux faux ordres de virement internationaux – où un malfrat convainc un salarié, au téléphone, de faire un important virement frauduleux – confirment leur repli entamé en 2014. Cependant, 145 sociétés en ont été victimes en 2018, pour un préjudice de 40 millions d'euros.

Le « chiffre noir »

Les piratages informatiques plus classiques, par exemple à des fins d'espionnage, sont toujours fréquents. La police et la gendarmerie en ont dénombré 9 970 en 2018, mais cette statistique a diminué de 9 % depuis 2016. Est-ce le signe d'une diminution de ce type d'attaque ? Impossible de le dire, affirment les auteurs du rapport, ce qui montre bien la difficulté qu'ont les services de l'Etat à mesurer finement la délinquance et la criminalité numérique.

Ainsi, police et gendarmerie ont enregistré 560 plaintes à la suite

à la disposition des enquêteurs sont parcellaires et alimentent un faux sentiment d'impunité

d'infections par un rançongiciel en 2018. Mais *« ce chiffre reste bien en deçà de la réalité des attaques. La majorité des entreprises victimes ne dépose pas plainte, ni même ne signale les faits aux forces de l'ordre, généralement pour préserver leur image »*, notent les auteurs. Même chose pour les fraudes à la carte bancaire : Perceval recueillerait moins de 20 % du nombre total de fraudes.

Mais l'outil statistique est aussi inadapté au phénomène « cyber » : seules certaines infractions (piratage, notamment) disposent d'une catégorie spécifique.

compte en propre. Il y a donc un important « chiffre noir » de la cybercriminalité. Au ministère de l'intérieur, on n'aime guère entendre l'expression. Elle traduit pourtant une réalité qui pose un problème d'efficacité dans la lutte contre ces phénomènes.

Les informations à la disposition des forces de l'ordre sont parcellaires, rendant plus difficiles encore les enquêtes et alimentant ainsi un faux sentiment d'impunité, qui lui-même décourage les victimes de porter plainte. Les enquêteurs se sont pourtant aperçus qu'ils pouvaient parvenir à de bons résultats en arrivant à faire des recoupements entre les affaires. La police nourrit beaucoup d'espoir dans le projet Thésée, qui doit permettre de centraliser et de relier entre elles des escroqueries dont le préjudice individuel est souvent en dessous du seuil à partir duquel les parquets ouvrent des enquêtes. ■

MARTIN UNTERSINGER

A Londres, le scandale financier de l'Euribor se dégonfle

un des accusés a été jugé non coupable, le 4 juillet. Un autre fait appel devant la Cour européenne des droits de l'homme

LONDRES - *correspondance*

'était censé être l'un des scandales symbolisant la crise financière. La nipulation de l'Euribor, un ux d'intérêt interbancaire uti-é comme référence pour des llions de produits financiers, lonné lieu à de nombreuses ndes contre les banques et a vert la voie à une série de pro-s spectaculaires à Londres. L'en-nte illicite entre les tradeurs, i se mettaient d'accord entre x pour déterminer le taux, a rvi d'illustration de la dérive s marchés d'avant-2008.

les onze accusés au début du processus judiciaire, seuls trois sont désormais en prison. Deux ont été jugés non coupables. Six ont refusé de se rendre au procès et ont, pour l'instant, tous remporté leur procès contre leur extradition.

Jeudi 4 juillet, Andreas Hauschild, un ancien de la Deutsche Bank, a été jugé non coupable, dans le troisième procès consacré à l'Euribor. Quelques jours plus tôt, le 25 juin, Philippe Moryoussef, un Français qui clame son innocence et a été condamné par contumace à huit ans de prison à Londres, a saisi la Cour européenne des droits de l'homme. Il estime que son procès a été

Le cas de M. Moryoussef, un ancien de Barclays, est le plus intéressant parce qu'il va au cœur de l'affaire. Pour faire simple, il reconnaît les faits, mais estime que les pratiques qu'on lui reproche ne constituent pas un délit. A l'époque, de 2005 à 2009, l'entente qui lui est reprochée était la pratique normale du marché et personne, ni chez ses supérieurs ni chez ses concurrents, n'y trouvait rien à redire. Selon lui, la loi qui le condamne est rétroactive car créée seulement après la crise. *« On essaie de faire croire aux contribuables qu'on est responsable de la crise. C'est la définition même du bouc émissaire »*, déclatian Bittar, de la Deutsche Bank, le duo central qui manipulait le taux. Les deux hommes sont français, se connaissaient bien et travaillaient tous les deux à la City au moment des faits.

Pratique devenu illégale en 2012

Chaque jour, l'Euribor était calculé en faisant la moyenne du taux interbancaire déclaré par quarante-huit banques. Le problème est que ce taux n'est pas scientifique. Les marchés évoluent en permanence et il est parfois discutable de savoir si le taux du moment est de 4,23 % ou 4,22 %, par exemple.

Jouant de cette zone grise, MM. Bittar et Moryoussef s'orga-

marge leurs positions sur les marchés. Pour l'accusation, cette entente est la preuve de la manipulation, d'autant qu'un changement d'un ou deux points de base pouvait rapporter des millions, étant donné les sommes en jeu.

Après avoir longtemps défendu en privé son innocence, M. Bittar a décidé de plaider coupable, à la surprise générale, en mars 2018. C'était une façon pour lui de réduire fortement sa peine, qui a finalement été de cinq ans de prison ferme. Pris au dépourvu, Philippe Moryoussef a failli le suivre dans sa démarche, avant de finalement décider de continuer la bataille judiciaire.

tous les jours n'était pas inventé, mais simplement l'évaluation du moment. D'autre part, rien ne lui interdisait de prendre en compte son propre intérêt commercial tant qu'il restait dans la zone grise, réaliste, des taux du moment. Selon lui, cette pratique était autorisée et courante. Ce n'est qu'en 2012 que la justice britannique, se penchant sur le Libor, un taux similaire, a décidé de déclarer cette pratique illégale. M. Moryoussef estime donc être victime d'une loi rétroactive. De plus, l'accusation n'a pas réussi à prouver d'enrichissement personnel lié à la manipulation. La Cour européenne des droits de l'homme va maintenant