Cybermenaces :
la transition numérique de la police

Par Olivier Ribaux et Thomas Souvignet

NDLR : cet article a été initialement publié dans la revue Third[1] en novembre 2020.

(1) https://third.digital/

Les transformations numériques de nos activités quotidiennes se sont inévitablement accompagnées d'une évolution de la criminalité et des menaces qui pèsent sur la société. Les cybermalveillances sont devenues quasi banales et nous ne prêtons même plus attention aux tentatives d'hameçonnage qui pullulent dans nos boîtes de « spam » (pourriels).

OLIVIER RIBAUX

Directeur de l'École des Sciences Criminelles de l'Université de Lausanne, Suisse.

THOMAS SOUVIGNET

Lieutenant-colonel de Gendarmerie (En disponibilité). Professeur à l'École des Sciences Criminelles de l'Université de Lausanne, Suisse.

Il devient alors indispensable de se demander comment les victimes ressentent ces attaques et y réagissent, et comment les pratiques policières évoluent pour s'adapter à ces transformations. Nous exprimerons ces enjeux et présenterons des développements opérationnels en illustrant nos propos par une fraude en ligne, typique, dont notre École a été la cible.

L'omniprésence des crimes numériques

Les transformations numériques de notre société engendrent toute sorte de nouveaux dangers qui perturbent concrètement notre quotidien. Ils sont mis en évidence dans l'étude menée en juin 2019 par l'Institut National de la Consommation pour Cybermalveillance.gouv.fr[2], le dispositif français d'assistance aux victimes, de prévention des

risques numériques et d'observation de la menace en France : plus de 9 français sur 10 admettent avoir déjà été confrontés à un acte de malveillance sur Internet.

Le nombre et la variété des évènements pour lesquels ce même organisme est sollicité[3] (Figure 1), indiquent le polymorphisme de ces dangers.

(2) https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/plus-de-9-francais-sur-10-ont-deja-ete-confrontes-a-un-acte-de-cybermalveillance.

(3) https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/chiffres-et-tendances-des-cybermenaces-cybermalveillance-gouv-fr-devoile-son-premier-rapport-dactivite-2019.

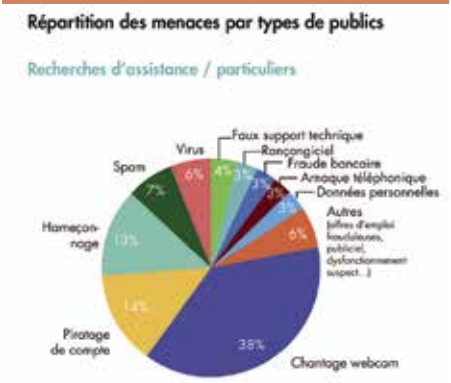

Figure 1 - Réparation des menaces lors des recherches d'assistance provenant de particuliers (source : www.cybermalveillance.gouv.fr).

Ces formes omniprésentes de criminalité en ligne, confirmées par d'autres entités comme l'association Signal Spam (Figure 2), sont souvent faussement considérées comme banales et bénignes. Elles sont néanmoins susceptibles de causer des dommages financiers et psychologiques parfois dramatiques pour les victimes.

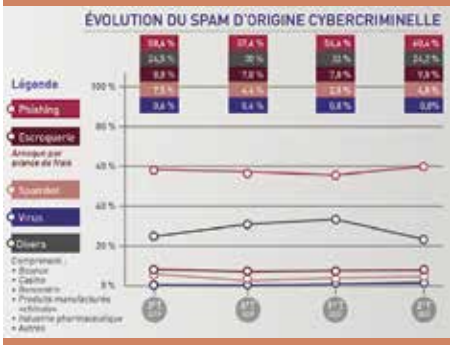

Figure 2 – Évolution du spam d'origine cybercriminelle entre 3ème trimestre 2019 et 2e trimestre 2020 (source : www.signal-spam.fr).

Dans son évaluation annuelle du paysage des cybermenaces pour l'année 2019 (IOCTA 2019[4]), Europol met notamment en avant les formes plus organisées et graves, telles que l'exploitation sexuelle de mineur en ligne, la fraude aux paiements, l'atteinte aux systèmes numériques (rançongiciel, compromission de données, etc.) ou encore les espaces numériques sur lesquels s'appuient des activités terroristes.

Nombre de ces cybermenaces ont toutefois un angle d'attaque commun :

(4) https://www.europol.europa.eu/activities-services/main-reports/internet

les vulnérabilités de l'humain. En effet, une action et une inattention de l'utilisateur sont très souvent nécessaires pour qu'une attaque puisse avoir l'effet escompté.

Au-delà des chiffres, comment réagir ?

Les réponses apportées jusqu'ici résultent d'une multitude d'initiatives souvent prometteuses, mais encore très fragmentées. Elles se confrontent à de nouvelles questions : qui doit prendre en charge les problèmes (institutions privées, publiques, responsabilité individuelle), quand (modes d'intervention) et comment (quelle répression ? quelles méthodes de prévention ?). Les questions éthiques (par ex. les libertés individuelles), comme le reste, doivent s'envisager à une nouvelle échelle.

Une attaque dont notre École a été victime durant l'été 2019, permet d'illustrer une partie de ces difficultés.

Nous prenons conscience qu'une attaque (détaillée dans un article publié dans *Forensic Science International : Digital Investigation*[5]) par harponnage (ou *spear phishing*) est en cours lorsque le premier auteur de cet article (professeur spécialisé en criminalistique numérique) reçoit, sur son adresse professionnelle, un courriel de son directeur (deuxième auteur de cet article) dont le sujet est « Hello are you available? ». Le tout est envoyé d'une adresse Gmail et non de celle de l'université. Tous deux sur nos lieux de vacances, nous arrivons toutefois à nous contacter et débute alors une gestion commune de l'incident.

(5) https://www.sciencedirect.com/science/article

Professionnels avertis en la matière, nous comprenons rapidement qu'il s'agit d'une usurpation d'identité (faux directeur) visant à demander de l'argent aux destinataires des courriels. Nous devons découvrir quels sont les destinataires de ceux-ci. Deux hypothèses se dessinent rapidement : soit le carnet d'adresse du Directeur a été piraté, soit l'attaquant a récupéré une liste de cibles de choix en exploitant des données publiées par exemple par le site web institutionnel de l'École.

Le mode opératoire étant défini, vient ensuite l'étape visant à endiguer l'attaque et, de manière pragmatique, éviter tout paiement. Nous comprenons que la fraude est synchrone (l'auteur dialogue en temps réel avec les personnes contactées). Notre réaction doit être immédiate.

Les messages étant envoyé d'une adresse Gmail créée par l'attaquant, la première idée consiste à s'appuyer sur Google. Un formulaire disponible sur le site support de Google semble pouvoir répondre au besoin. Mais, en restant réaliste, nous comprenons que le temps de réaction du géant américain n'est pas compatible avec l'évolution de la fraude.

L'identification des destinataires n'étant toujours pas possible, le directeur prend la décision :

- d'envoyer un courriel à l'ensemble des collaborateurs de l'École,

- d'informer le support informatique de l'université,

- de prendre contact individuellement avec quelques adresses de sa propre liste de contacts, en dehors de l'École, pour tester l'hypothèse du piratage de son compte.

Enfin, le directeur contacte officieusement quelques responsables de la police locale, spécialisés en numérique, afin de connaître la démarche à suivre.

Les actions menées ont eu l'effet escompté puisque certains collaborateurs en discussion avec l'attaquant ont stoppé net à réception du courriel adressé aux collaborateurs de l'École. De même, le service informatique de l'université a été en mesure d'intercepter immédiatement le flux continu de messages provenant de l'attaquant. Par les retours obtenus des collaborateurs et les réponses des contacts hors de l'université, il apparaît maintenant clairement que le cercle des personnes ciblées se restreint aux membres de l'École.

Dans une seconde phase d'analyse à froid, cette hypothèse a été confirmée par l'examen des journaux d'événement (logs) du site internet de l'École : des accès aux adresses électroniques des collaborateurs par le site internet étaient synchronisés avec l'émission des courriels d'harponnage.

Finalement, seule une cible sur une centaine ira jusqu'à la phase de paiement, mais ce paiement sera annulé à la dernière minute.

Dans cette situation assez simple, de nombreuses décisions et démarches, à des niveaux différents ont été nécessaires pour endiguer la fraude.

Ces démarches, pas forcément simples ou accessibles, même pour des utilisateurs avertis, montrent la difficulté de faire face à une attaque technologiquement simple. On peut aisément imaginer la grande difficulté d'une victime âgée face à un rançongiciel (eg. *cryptolocker*) ou une prise en main à distance lors d'une fraude au faux support technique.

Une évolution nécessaire de la réponse policière

Cet exemple met en exergue un paradoxe quant à la manière dont la Police aborde la criminalité sur Internet et aux attentes que nous avons à l'égard de cette institution.

En effet, si nous n'avions pas été victime d'une attaque en ligne mais d'une rixe ou d'un cambriolage, nous aurions immédiatement appelé la Police et lui aurions laissé entièrement gérer la crise engendrée. Dans son rôle régalien, celle-ci aurait sans doute réalisé des opérations de police

technique et scientifique, effectué une enquête de voisinage et saisi les images de vidéoprotection disponibles. Quand bien même nous enseignons à nos étudiants ces pratiques, nous aurions entièrement « confié » ces opérations à la Police.

Dès lors, pourquoi n'avons-nous pas agi de la même manière avec cette cyberattaque dont nous avons été victimes ? Parce que nous n'avions pas « confiance » en la réponse que pourrait apporter la Police dans un délai aussi court. Même dans un contexte de confiance Police-Nation aussi fort qu'en Suisse, où la Police est régulièrement sollicitée pour des renseignements de toutes natures, nous considérions tacitement qu'elle n'aurait pas les ressources pour traiter immédiatement notre petite attaque. N'aurait-elle pas agi immédiatement si l'on tentait de s'en prendre à nos biens dans le monde physique ?

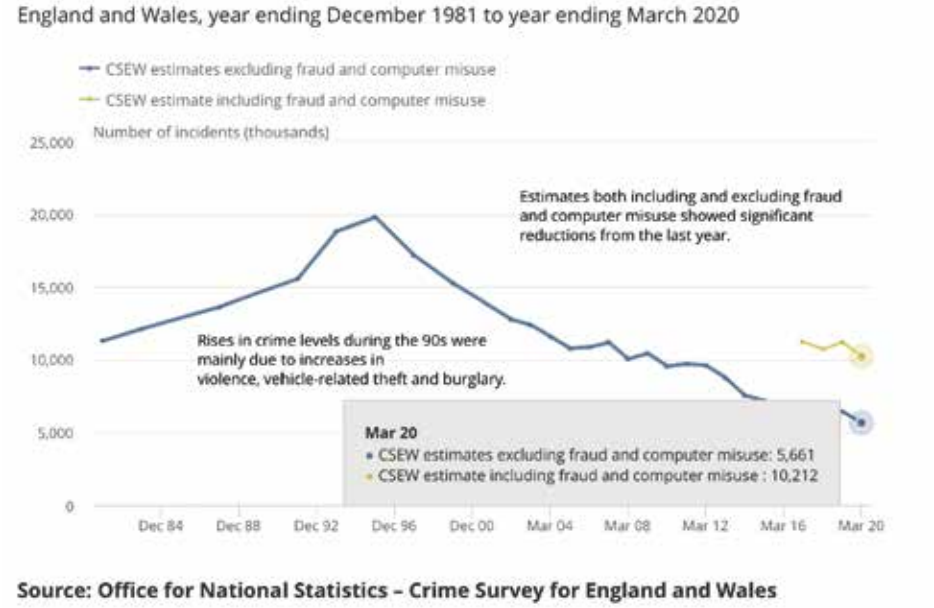

Figure 3 – Estimation de la délinquance en Angleterre et Pays de Galle (source : Office nationale de la statistique du Royaume-Uni[6]).

Cela pose ainsi la nécessité et la capacité des forces de l'ordre à traiter individuellement toutes les cyberattaques.
Une enquête doit-elle et peut-elle être menée dès la réception d'une tentative d'hameçonnage ? Si ce n'est pas le cas, à partir de quel niveau d'intensité une réponse policière doit-elle être apportée ?

Pour comprendre l'éventuelle difficulté à faire face à ces cyberattaques, il suffit de consulter les statistiques de la délinquance de l'Angleterre et du Pays de Galles (Figure 3). En effet, la prise en compte des crimes et délits liés au numérique depuis 2007 a pour effet de quasiment doubler la délinquance estimée.

Au vu de la criminalité dans les années 1990-2000, on pourrait se dire, qu'à effectif du même ordre de grandeur[7], la moitié serait dédiée à cette nouvelle délinquance et qu'une réponse à la hauteur de la criminalité traditionnelle serait produite. Ceci n'est bien sûr pas le cas.

Dès lors, les polices sont-elles atteintes du « syndrome Kodak » qui semble frapper les laboratoires forensiques[8] ? En d'autres termes, est-ce que les forces de police ont su prendre le virage numérique, adapter leurs pratiques aux cybermenaces ? Faute de prendre en compte ces nouvelles menaces, et campant sur des pratiques du siècle dernier, ne risquent-elles pas, à l'image de Kodak qui misait tout sur la vente de pellicules, de ne pas se remettre de ces évolutions numériques ?

Tout d'abord, il est possible d'argumenter à ceux qui voient un « syndrome Kodak » dans l'adaptation des forces de police aux cybermenaces, qu'un « syndrome Polaroid » peut également être mis en avant. En effet, même avec l'avènement du numérique les pratiques traditionnelles restent d'actualité. Le succès du Polaroid ne se dément pas, comme celui de la criminalité traditionnelle.

Ensuite, les forces de l'ordre s'attachent à réaliser leurs transformations numériques. En France, dès la fin du XX^{e} siècle, les spécialistes en scène de crime[9] ont été rejoints par des spécialistes en analyse de supports et en enquêtes numériques[10].

(6) https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2020.

(7) https://www.gov.uk/government/collections/police-workforce-england-and-wales

(8) https://onlinelibrary.wiley.com/doi/abs/10.1111/1556-4029.13849.

(9) Technicien en Identification Criminelle – TIC – en Gendarmerie et Agent spécialisé de Police Technique et Scientifique – ASPTS – en Police.

(10) Enquêteur spécialisé en technologie numérique – NTech – en Gendarmerie et Investigateurs en cybercriminalité – ICC – en Police.

Depuis 2009[11], la Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements (PHAROS) a quant-à-elle pour mission de recueillir, de manière centralisée, l'ensemble des signalements de nombreux faits commis en ligne, dont les escroqueries et arnaques financières utilisant internet.
Enfin des unités spécialisées détiennent les compétences techniques nécessaires à la lutte contre les fraudes mettant en œuvre des technologies évoluées, comme le montre le démantèlement d'un réseau de *Darkphone* (téléphones hautement sécurisés utilisés par des groupes criminels) par la Gendarmerie Nationale[12].

(11) https://www.legifrance.gouv.fr/affichTexte.do?cidTexte

(12) https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

Reste tout de même la prise en compte de l'utilisateur qui doit faire face à une cyberattaque, telle que nous l'avons vécue. Là encore, les agences gouvernementales françaises prennent en compte le virage numérique avec esprit d'innovation.

La Gendarmerie a ouvert une brigade en ligne, accessible 24h/24 en créant la « brigade numérique ». La coproduction de sécurité est ainsi régulièrement utilisée dans les mécanismes mis en place. Nous noterons ainsi la participation des forces de l'ordre dans des associations de lutte contre la criminalité numérique (Signal Spam, CECyF, etc.) ou encore la création de Groupes d'Intérêt Public (GIP) comme le GIP Action contre la Cybermalveillance (GIP ACYMA) derrière « cybermalveillance.gouv.fr » préalablement cité.

Une marge de manœuvre encore grande

Malgré cette prise en compte des nouvelles menaces portées par le numérique et la transformation de leurs pratiques, les forces de Police ont quand même du chemin à parcourir pour prendre en compte la criminalité numérique comme elles prennent en compte la criminalité traditionnelle.
En dehors d'une meilleure prise en charge des victimes, l'exploitation systématique du renseignement judiciaire pourrait être un moyen efficace de rattraper ce retard. C'est du moins ce qu'essaie de faire la Suisse en développant la Plateforme d'Information de la Criminalité Sérielle en Ligne (PICSEL). Cette plateforme exige déjà des policiers qui saisissent les plaintes et qui alimentent le dispositif, une attention particulière à ces formes de criminalité jusqu'ici ignorées. Ils doivent s'entretenir avec le plaignant et s'appuyer

sur les brigades spécialisées pour exprimer clairement le mode opératoire et en identifier des traits pertinents. Les traces accessibles sont aussi susceptibles d'aider à détecter des problèmes répétitifs et à suivre leur évolution. L'analyse des informations, ainsi réunies et organisées, offre les moyens d'adapter les stratégies préventives et répressives, de mieux communiquer avec les partenaires et avec le public, de prioriser les efforts et d'orienter les enquêtes. En moins de deux ans de fonctionnement et bien qu'en état encore embryonnaires, ces nouveaux processus ont déjà modifié profondément l'approche policière des crimes transformés numériquement.

L'AUTEUR

Lieutenant-Colonel de gendarmerie en position de disponibilité, Thomas Souvignet est professeur spécialisé en traces numériques à l'École des Sciences Criminelles de l'Université de Lausanne. Titulaire de différents masters (Sécurité des Systèmes d'Information — Information Security and Computer Crime — Systèmes embarqués et mobiles), il détient un doctorat en Informatique (sujet relatif à la lutte contre la fraude aux moyens de paiement). Après avoir œuvré au développement du département informatique-électronique de l'IRCGN pendant une douzaine d'années, il se consacre actuellement à élargir la recherche, l'expertise et l'enseignement du numérique au sein de la plus ancienne école de police scientifique au monde.