INTERPOL

CYBERCRIMINALITÉ :

IMPACT DU COVID-19

AOÛT 2020

© INTERPOL 2020
Secrétariat général d'INTERPOL
200, quai Charles de Gaulle
69006 Lyon
France

Web: www.interpol.int
E-mail: info@INTERPOL.int

TABLE DES MATIÈRES

Introduction **4**

Évolution des tendances et menaces en matière de cybercriminalité durant le COVID-19 **6**

Tendances régionales de la cybercriminalité **6**

AFRIQUE 6

AMÉRIQUES 6

ASIE ET PACIFIQUE SUD 6

EUROPE 7

MOYEN-ORIENT ET AFRIQUE DU NORD 7

Les principales cybermenaces liées au COVID-19 **8**

ESCROQUERIES EN LIGNE ET HAMEÇONNAGE 8

LOGICIELS MALVEILLANTS VISANT À DÉSORGANISER (RANÇONGICIELS ET ATTAQUES PAR DÉNI DE SERVICE DISTRIBUÉ 9

LOGICIELS MALVEILLANTS VISANT À OBTENIR DES DONNÉES 10

DOMAINES MALVEILLANTS 11

MÉSINFORMATION 12

La réponse d'INTERPOL **14**

Priorités et recommandations **16**

Prévisions à court terme **18**

Conclusion **19**

INTRODUCTION

Cette pandémie de coronavirus sans précédent a de profondes répercussions sur les cybermenaces dans le monde. Une crise sanitaire mondiale doublée d'une augmentation considérable des activités cybercriminelles liées au COVID-19 met à rude épreuve les communautés des services chargés de l'application de la loi. Selon l'un des partenaires d'INTERPOL appartenant au secteur privé, 907 000 messages non sollicités, 737 incidents liés à des logiciels malveillants et 48 000 URL malveillantes – tous en rapport avec le COVID-19 – ont été détectés entre janvier et le 24 avril 2020[1].

Afin de causer le plus grand préjudice possible et d'augmenter le plus possible leurs profits, les cybercriminels s'intéressent moins aux particuliers et aux petites entreprises et se tournent vers les grandes sociétés, les gouvernements et les infrastructures essentielles qui jouent un rôle fondamental dans la réponse à la flambée épidémique. Dans le même temps, du fait du passage soudain et nécessaire au télétravail partout dans le monde, les entreprises ont dû déployer très vite des systèmes distants, des réseaux et des applications, et les malfaiteurs exploitent les vulnérabilités accrues en matière de sécurité qu'engendre le travail à distance pour dérober des données, générer des profits et provoquer des perturbations.

Compte tenu de cette situation, la Direction de la Cybercriminalité d'INTERPOL a élaboré le présent Rapport d'évaluation mondial portant sur la cybercriminalité liée au COVID-19 en s'appuyant sur l'accès exceptionnel aux données de 194 pays membres et de partenaires privés dont elle bénéficie afin de brosser un tableau complet de la cybercriminalité au temps de la pandémie. Ce rapport est basé sur les données communiquées par les pays membres et les partenaires privés d'INTERPOL dans le cadre de l'Enquête mondiale sur la cybercriminalité menée par l'Organisation en avril et mai 2020. Quarante-huit de ses 194 pays membres ont répondu à cette enquête, tandis que 4 de ses 13 partenaires privés ont communiqué leurs données aux fins de l'établissement du présent document.

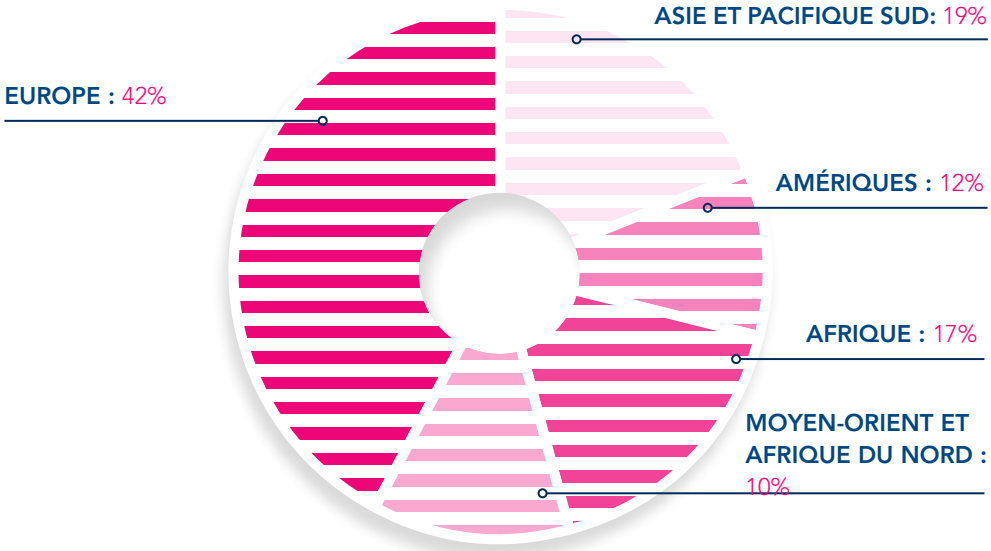

Fig. 1 - Enquête mondiale INTERPOL sur la cybercriminalité :
répartition géographique des pays ayant répondu

[1] Trend Micro, informations consultées et extraites le 27 mai 2020 à l'adresse https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

L'analyse qui en a été tirée a été complétée par des informations fournies par les partenaires du secteur privé et les Groupes de travail régionaux de lutte contre la cybercriminalité d'INTERPOL. Le présent rapport inclut également des informations et analyses de l'unité de la Réponse aux cybermenaces d'INTERPOL (CTR) et du Centre de fusionnement sur la cybercriminalité (CFC) de l'Organisation – une équipe basée à Singapour, qui réunit des experts des services chargés de l'application de la loi et du secteur privé. Les principales constatations concernant la cybercriminalité liée à la pandémie de COVID-19 sont les suivantes :

- **Escroqueries en ligne et hameçonnage**
  Voyant dans la pandémie une occasion d'accroître les chances de succès de leurs attaques, les acteurs de la menace ont adapté leurs activités d'escroquerie et d'hameçonnage en ligne habituelles. En ayant recours à des e-mails ayant pour objet le COVID-19, dans lesquels ils prétendent souvent appartenir à des autorités gouvernementales et sanitaires, ils incitent leurs victimes à communiquer des données à caractère personnel et à télécharger des contenus malveillants.

- **Logiciels malveillants visant à désorganiser (rançongiciels et attaques par déni de service distribué)**
  Les cybermalfaiteurs déploient de plus en plus fréquemment des logiciels malveillants contre des infrastructures et établissements de santé essentiels en raison de l'ampleur des conséquences potentielles et des bénéfices pouvant être engrangés. Ces attaques par rançongiciel ou déni de service distribué peuvent se traduire par des perturbations régulières ou un arrêt total de l'activité, ainsi que par une perte temporaire ou permanente d'informations critiques.

- **Logiciels malveillants visant à obtenir des données**
  On enregistre également une hausse des déploiements de logiciels malveillants tels que les chevaux de Troie contenant un outil de prise de contrôle à distance, les voleurs d'informations, les logiciels espions et les chevaux de Troie bancaires. Utilisant comme appât des informations liées au COVID-19, les acteurs de la menace infiltrent les systèmes afin de compromettre des réseaux, dérober des données, détourner des fonds et constituer des botnets.

- **Domaines malveillants**
  Du fait de la demande accrue de fournitures médicales et d'informations sur le COVID-19, on a constaté une hausse importante du nombre de cybermalfaiteurs enregistrant des noms de domaine contenant des mots clés en lien avec celui-ci, comme « coronavirus » ou « COVID ». Ces sites Web frauduleux sont utilisés dans le cadre de très nombreuses activités malveillantes, notamment des serveurs C2, le déploiement de logiciels malveillants et l'hameçonnage.

- **Mésinformation**
  Les mésinformations et les fausses informations, de plus en plus nombreuses, se répandent rapidement dans le public. Alimentées par les incertitudes de la situation sociale et économique dans le monde, les informations non confirmées, les menaces mal comprises et les théories du complot ont contribué à l'anxiété des populations et, dans certains cas, facilité l'exécution de cyberattaques.

ÉVOLUTION DES TENDANCES ET MENACES EN MATIÈRE DE CYBERCRIMINALITÉ DANS LE CONTEXTE DU COVID-19

Tendances régionales de la cybercriminalité

Si la cybercriminalité connaît un pic dans le monde durant la pandémie de COVID-19, les tendances en la matière varient d'une région à l'autre. La section ci-dessous donne un aperçu de la cybermenace liée au COVID-19 sur le plan régional.

AFRIQUE

- Les pays membres africains ayant répondu à l'enquête ont souligné que, du fait du recours accru aux paiements électroniques ou sans numéraire dès le début de la pandémie, le public avait été plus exposé aux cyberattaques.
- Alors que la plupart des organismes et entreprises ont mis en place une politique de télétravail, les vulnérabilités de ces systèmes ont entraîné une hausse importante de l'hameçonnage, des sextorsions et des escroqueries aux dons dont le thème avait été choisi en conséquence.
- La circulation de fausses informations concernant le COVID-19 dans les médias sociaux a augmenté.
- L'activité relativement faible des partenariats public-privé visant à combattre la cybercriminalité a contribué à la hausse du nombre de cyberinfractions non résolues.

AMÉRIQUES

- Les pays ayant répondu ont fait état d'une hausse importante des campagnes d'hameçonnage et d'escroquerie ayant pour thème le COVID-19 et exploitant la crise du coronavirus et le confinement qui s'en est suivi.
- De nombreuses entreprises des Amériques ayant fait appel au télétravail, les cybermalfaiteurs ciblent de plus en plus leurs employés afin de prendre le contrôle des systèmes par un accès à distance aux réseaux d'entreprise, dans le but de dérober des informations sensibles.
- Une campagne de rançongiciels passant principalement par le logiciel malveillant LOCKBIT touche actuellement des entreprises de taille moyenne de certains pays de la région.
- Les malfaiteurs utilisent de plus en plus les médias sociaux aux fins d'exploitation sexuelle des enfants sur Internet. Les délinquants pédosexuels des réseaux spécialisés repèrent et contactent en particulier leurs victimes sur ces médias, en tirant parti du confinement mondial. Parallèlement, le commerce d'images représentant des faits d'exploitation sexuelle d'enfants s'est intensifié.

ASIE ET PACIFIQUE SUD

- Les principales tendances de cette région concernent les campagnes d'escroquerie et d'hameçonnage liées au COVID-19 ainsi que la vente illégale en ligne de fournitures médicales, de médicaments et d'équipements de protection individuelle de contrefaçon.

- Les cybermalfaiteurs exploitent les vulnérabilités des outils de téléconférence.
- La plupart des pays membres de la région qui ont participé à l'enquête ont fait état de la circulation de fausses informations et mésinformations liées au COVID-19.
- Une prise de conscience insuffisante des problèmes de cybersécurité et l'absence d'«hygiène » en la matière ont été citées comme faisant partie des principaux défis de la région.

EUROPE

- Deux tiers des pays membres européens ont signalé une hausse importante du nombre de domaines malveillants enregistrés avec les mots clés « COVID » ou « corona » pour tirer parti de l'augmentation des recherches en ligne d'informations concernant le COVID-19.
- Les cybermalfaiteurs utilisent la pandémie pour déployer des rançongiciels ciblant des infrastructures et des établissements de santé essentiels, chargés de lutter contre le COVID19.
- Le clonage de sites gouvernementaux officiels en vue de dérober les données sensibles des utilisateurs, susceptibles d'être ensuite utilisées dans le cadre de cyberattaques, est de plus en plus fréquent.
- Les services européens chargés de l'application de la loi ont noté l'existence de très nombreuses campagnes d'hameçonnage.

MOYEN-ORIENT ET AFRIQUE DU NORD

- Cette région a signalé le recours croissant aux médias sociaux pour diffuser de fausses informations liées au COVID19.
- Les plateformes de médias sociaux sont fréquemment utilisées pour la vente illicite de produits pharmaceutiques et parapharmaceutiques liés au coronavirus.
- Augmentation des enregistrements de domaines malveillants prétendant fournir des statistiques sur le COVID19.
- Augmentation du nombre d'hameçonnages et d'escroqueries en ligne liés à la pandémie de COVID19.

LES PRINCIPALES CYBERMENACES LIÉES AU COVID19

À partir de l'analyse approfondie des données reçues des pays membres, des partenaires privés et du Centre de fusionnement sur la cybercriminalité (CFC), nous avons déterminé que les principales menaces liées à la pandémie de COVID19 étaient les suivantes :

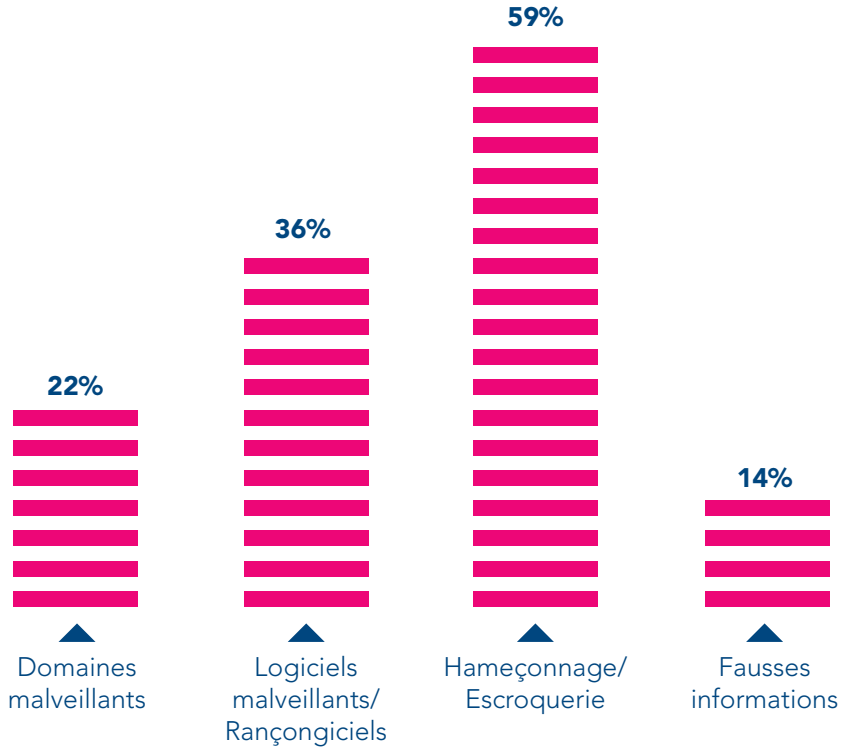

Fig. 2 - Répartition des principales cybermenaces liées aux COVID-19 d'après les réponses fournies par les pays membres

Escroquerie en ligne et hameçonnage

Deux tiers environ des pays membres ayant répondu à l'enquête ont signalé un recours important à des thèmes en rapport avec le COVID-19 aux fins d'hameçonnage et d'escroquerie sur Internet depuis le début de l'épidémie[2]. Depuis janvier 2020, l'un des partenaires privés d'INTERPOL, Trend Micro, a ainsi détecté 907 000 messages liés à ce sujet. Tirant parti du ralentissement de l'activité économique et de l'anxiété éprouvée par la population durant la pandémie, les cybermalfaiteurs ont perfectionné leurs tactiques d'ingénierie sociale en basant leurs attaques sur le COVID-19[2]. De nombreux groupes criminels organisés existants se sont en particulier mis à exploiter les informations relatives à la situation de la pandémie et les pénuries ; ils ont également fait de la publicité pour des médicaments, des mesures fiscales et des aides d'urgence qui étaient faux.

[2] Trend Micro, informations consultées et extraites le 19 avril 2020 à l'adresse https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

Une grande partie des incidents signalés aux autorités chargées de l'application de la loi concernait l'envoi d'e-mails d'hameçonnage ayant trait au COVID-19 pour obtenir des données d'identification et des mots de passe d'utilisateurs. Ces e-mails étaient souvent censés émaner d'autorités gouvernementales ou sanitaires officielles fournissant des informations et des recommandations concernant la pandémie. Au-delà de ces liens directs avec les actualités relatives à la situation, Kaspersky, partenaire d'INTERPOL, a signalé que des acteurs de la menace prétextaient un remboursement d'impôts lié au COVID-19 pour attirer les bénéficiaires sur un site Web frauduleux recueillant les données financières et fiscales d'utilisateurs sans méfiance.

Des e-mails d'hameçonnage soi-disant envoyés par des ministères de la Santé ou l'Organisation mondiale de la santé contenaient des pièces jointes qui exploitaient les vulnérabilités pour exécuter un code malveillant. Les pays membres d'INTERPOL ainsi que ses partenaires privés ont signalé que l'utilisation de logiciels malveillants tels qu'Emotet, Trickbot et Cerberus, conçus spécifiquement dans le but de dérober des informations, était très répandue dans les e-mails d'hameçonnage.

Des informations communiquées par des partenaires privés indiquent que les escroqueries aux faux ordres de virement ont toujours la préférence de nombreux acteurs de la menace. Ces derniers ont adapté leurs tactiques au contexte actuel du COVID-19 – usurper les adresses e-mail de fournisseurs et de clients, ou utiliser des adresses quasi identiques aux leurs – pour mener des attaques. Le besoin pressant de produits de première nécessité et de produits de santé constitue pour les malfaiteurs une occasion idéale de récupérer des informations ou de détourner vers des comptes illicites des millions de dollars destinés aux approvisionnements.

D'après les informations fournies par les pays membres et les partenaires privés, les principaux types d'hameçonnage liés au COVID-19 sont les suivants :

- E-mails provenant d'autorités sanitaires nationales ou mondiales ;
- Instructions gouvernementales et initiatives en matière d'aides financières ;
- Fausses demandes de paiement et de remboursement ;
- Offres de vaccins et de fournitures médicales ;
- Applications de traçage pour téléphone portable liées au COVID-19 ;
- Offres de placements et d'actions ;
- Demandes de dons liées au COVID-19.

Globalement, avec le COVID-19 et le confinement qui a suivi, les hameçonnages en lien avec le coronavirus se développent. Ils exploitent les peurs, éveillent l'intérêt des personnes vulnérables et tirent parti des perturbations dans le monde du travail.

LOGICIELS MALVEILLANTS VISANT À DÉSORGANISER (RANÇONGICIELS ET ATTAQUES PAR DÉNI DE SERVICE DISTRIBUÉ)

Les attaques par logiciels malveillants se sont adaptées à la flambée de coronavirus ; elles sont plus nombreuses et leurs cibles changent. Comme le montre l'analyse du CFC et l'appui

fourni par celui-ci aux pays membres, les campagnes faisant appel à des logiciels malveillants visant à désorganiser ciblent désormais davantage les organismes gouvernementaux et le secteur de la santé, dont il est possible d'exiger plus d'argent, que les particuliers et les petites entreprises.

Plusieurs pays membres ont signalé des attaques par logiciels malveillants contre les infrastructures essentielles d'organismes gouvernementaux, d'hôpitaux et de centres médicaux totalement débordés du fait de la crise sanitaire. Ces attaques par rançongiciel ou par déni de service distribué ont pour but de rendre les données inaccessibles ou de perturber le système, aggravant ainsi une situation déjà extrêmement tendue.

Selon le CFC, au cours des deux premières semaines d'avril 2020, on a enregistré un pic d'attaques par rançongiciel menées par plusieurs groupes relativement peu actifs les mois précédents. Cela signifie que des établissements où le rançongiciel n'a pas encore été activé ont peut-être été touchés. Les enquêtes des services chargés de l'application de la loi indiquent qu'après avoir procédé à une reconnaissance minutieuse du réseau des entités ciblées, les attaquants ont estimé avec une grande précision la rançon maximale qu'ils pouvaient réclamer. Lorsque le rançongiciel est déployé en des points stratégiques du réseau, là où il peut perturber le plus l'activité, les structures visées sont souvent contraintes de verser cette rançon. Ces attaques peuvent être combinées avec l'exfiltration d'informations sensibles, utilisées par la suite pour renforcer la pression exercée en vue d'obtenir un paiement.

Les principales familles de rançongiciels récemment détectées par les partenaires privés d'INTERPOL sont CERBER, NetWalker et Ryuk. Elles évoluent en permanence pour accroître les dommages pouvant être provoqués par une attaque ainsi que les profits générés pour ses auteurs.

À l'instar des campagnes de propagation de rançongiciels, les attaques par déni de service distribué signalées au CFC ont pris de l'ampleur et visent à perturber le fonctionnement de diverses entités et services essentiels. En surchargeant les portails de services en ligne avec un trafic supérieur à celui que le serveur ou le réseau peuvent traiter, les cybermalfaiteurs menacent de rendre indisponibles les sites Web ciblés s'il n'est pas procédé à un virement à leur profit.

Les conséquences des attaques par rançongiciel et déni de service distribué varient et peuvent aller de la perturbation du fonctionnement au blocage de systèmes essentiels et à la perte de données qui s'accompagnent de préjudices financiers dus à l'immobilisation puis à la restauration des systèmes et fichiers.

DOMAINES MALVEILLANTS

Plus d'un tiers des pays membres relèvent un nombre croissant de nouveaux domaines enregistrés avec les mots clés « COVID » ou « Corona ». Comme pour les campagnes d'hameçonnage ayant trait au COVID-19, un pourcentage élevé de domaines prétendant fournir des informations, des statistiques ou des systèmes de traçage relatifs à cette maladie est utilisé pour toute une palette d'activités malveillantes qui tirent parti de la soif d'information du public durant la pandémie. À la fin mars 2020, 116 357 nouveaux domaines enregistrés liés au COVID-19 avaient été détectés, dont 2 022 considérés comme malveillants et 40 261 comme présentant un « risque élevé »[3].

[3] Palo Alto Networks, informations consultées et extraites le 6 juillet 2020 à l'adresse https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

En juin 2020, le Groupe spécial mondial sur les domaines malveillants de la Direction de la Cybercriminalité d'INTERPOL avait repéré et analysé 200 000 domaines de ce type concernant 80 pays membres.

Soit les nouveaux domaines malveillants enregistrés hébergent des logiciels malveillants servant à obtenir des données, soit ils ont pour but de recueillir des données à caractère personnel, les victimes étant contactées par l'intermédiaire de campagnes d'e-mails, de SMS ou d'appels téléphoniques non sollicités. Entre février et mars 2020, Palo Alto Networks, l'un des partenaires privés d'INTERPOL, a relevé une augmentation de 569 % des enregistrements malveillants, associés notamment à des logiciels malveillants et à l'hameçonnage, et une hausse de 788 % des enregistrements présentant un risque élevé, par exemple d'escroquerie, de minage pirate, et concernant des domaines associés à des URL malveillantes. Cette augmentation des enregistrements a fait suite, avec un décalage de quelques jours, au pic d'intérêt pour les sujets liés au COVID-19 dans Google Trends[4].

D'autres informations reçues des services chargés de l'application de la loi montrent que certains sites Web malveillants ont été créés afin d'imiter ceux de services publics officiels comme les portails gouvernementaux, ceux d'entreprises de télécommunications, de banques, d'autorités fiscales et douanières nationales, etc. Cette tendance a été mise en évidence dans un pays membre où une initiative nationale visant à fournir rapidement un soutien financier aux travailleurs indépendants et aux petites entreprises a été exploitée. Pour bénéficier de cette assistance, les entreprises devaient faire leur demande sur un site officiel du gouvernement. Les acteurs de la menace ont très vite copié les sites concernés et déployé une fausse application pour recueillir les données à caractère personnel fournies par les demandeurs.

Un autre sujet de préoccupation réside dans l'augmentation du nombre de sites Web frauduleux qui exploitent la forte hausse de la demande de masques chirurgicaux, d'équipements de protection individuelle, de kits de dépistage du coronavirus et de respirateurs pour héberger un commerce illicite portant sur ces fournitures de première importance. Les tactiques des propriétaires de ces sites varient : copie d'un site légitime, vente d'articles non autorisés ou de marchandises de contrefaçon, ou encore non-livraison d'articles pourtant payés. Un problème se pose par ailleurs lorsque l'argent versé par les victimes de ce commerce illégal est envoyé sur des comptes bancaires à l'étranger, car il devient dès lors difficile d'attribuer l'infraction à son auteur et de recouvrer le montant payé.

LOGICIELS MALVEILLANTS VISANT À OBTENIR DES DONNÉES

L'Enquête mondiale sur la cybercriminalité a mis en évidence un important recours aux logiciels malveillants visant à obtenir des données en trompant les victimes sous couvert d'informations liées au COVID-19. Les acteurs de la menace incitent les utilisateurs à exécuter ces logiciels de type cheval de Troie contenant un outil de prise de contrôle à distance, voleur d'informations, logiciel espion[5] ou cheval de Troie bancaire afin de compromettre des réseaux, de recueillir

[4] Palo Alto Networks, informations consultées et extraites le 24 avril 2020 à l'adresse https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

[5] Group IB, informations consultées et extraites le 26 avril 2020 à l'adresse https://www.group-ib.com/media/covid-phishing-campaings/

des données, de détourner des fonds et de constituer des botnets. La propagation de ces fichiers exécutables malveillants est grandement facilitée par les campagnes d'hameçonnage liées au COVID-19. On a également observé que les logiciels malveillants étaient téléchargés via des liens intégrés à des cartes géographiques interactives concernant le coronavirus, des applications thématiques et des sites Web frauduleux.

Parmi les logiciels malveillants visant à obtenir des données que nous ont signalés nos partenaires privés, Emotet constitue l'un des exemples les plus caractéristiques. Sa prolifération s'est considérablement renforcée depuis le début de la pandémie. Les chercheurs d'IBM X-Force ont détecté au Japon un cheval de Troie Emotet qui était largement utilisé par des cybermalfaiteurs se faisant passer pour des prestataires de services destinés aux personnes handicapées[6]. Dans leurs emails d'hameçonnage, les acteurs de la menace incitaient leurs victimes à ouvrir des pièces jointes censées présenter des mesures de prévention contre le COVID-19, mais qui était infectées par Emotet. De nombreuses personnes sont tombées dans le piège car les messages semblaient émaner du compte de messagerie officiel du prestataire de service et contenaient apparemment une adresse et un numéro de téléphone authentiques. En enquêtant sur la même affaire, les chercheurs de Kapersky ont découvert que le cheval de Troie Emotet était généralement envoyé aux formats .pdf, .mp4 et .docx sous forme de pièce jointe à des e-mails contenant soi-disant des renseignements utiles sur le coronavirus, notamment les informations les plus récentes, les mesures de protection et les méthodes de détection[7]. Ces attaques se sont avérées particulièrement efficaces car les cybermalfaiteurs ont choisi le bon moment – les gens étant anxieux et inquiets – pour diffuser ce logiciel malveillant. Une quantité importante de données à caractère personnel a par conséquent été dérobée ces derniers mois. Ayant affecté 13 % des organisations dans le monde, Emotet arrivait en janvier 2020 au premier rang des familles de logiciels malveillants visant à obtenir des données[8].

Trickbot est un autre exemple de logiciel malveillant de ce type dont la prolifération s'est considérablement renforcée en raison de la pandémie. D'après une étude récente de Microsoft, il s'agit du logiciel malveillant le plus souvent associé à des incitations liées au coronavirus[9]. Depuis le début de la pandémie, aucun autre logiciel malveillant n'aurait aussi souvent été utilisé avec des emails d'hameçonnage. Il a également été envoyé à des victimes sous forme de pièces jointes à des emails émanant d'un faux organisme à but non lucratif proposant des tests gratuits de dépistage du COVID19.

[6] IBM, informations consultées et extraites le 24 avril 2020 à l'adresse https://exchange.xforce.ibmcloud.com/collection/18f373debc38779065a26f1958dc260b

[7] https://www.techrepublic.com/article/hackers-using-coronavirus-scare-to -spread-emotet-malware-in-japan/

[8] Check Point Technologies, informations consultées et extraites le 6 juillet 2020 à l'adresse https://blog.checkpoint.com/2020/02/13/january-2020s-most-wanted-malware-coronavirus-themed-spam-spreads-malicious-emotet-malware/

[9] https://twitter.com/MsftSecIntel/status/1251181180281450498

MÉSINFORMATION

À la mi-février 2020, l'Organisation mondiale de la santé (OMS) a annoncé que le COVID19 s'accompagnait d'une « infodémie » de mésinformation. L'agence des Nations Unies a appelé l'attention sur le fait que la mésinformation concernant la pandémie présentait un risque grave, dont la dangerosité s'apparentait à celle du virus lui-même[10].

D'après une étude mondiale menée par le Reuters Institute, les thèmes les plus fréquents liés au coronavirus qui ressortent des fausses nouvelles et des mésinformations qui se sont multipliées sont les suivants[11]:

- L'action des autorités publiques ;
- La propagation dans la population ;
- Les informations médicales d'ordre général ;
- Les acteurs de premier plan ;
- Les théories du complot ;
- Le mode transmission du virus ;
- La préparation de la population ;
- La mise au point d'un vaccin.

Vingt-sept pour cent des pays ayant participé à l'Enquête mondiale sur la cybercriminalité ont confirmé la circulation de fausses informations liées au COVID-19 dans la population, et 21 % ont fait état de leur préoccupation croissante concernant cette tendance. En l'espace d'un mois, un pays membre a signalé 290 publications et, dans la plupart des cas, celles-ci dissimulaient un logiciel malveillant.

Les informations ont principalement été partagées via les médias sociaux (WhatsApp, Facebook, Twitter, etc.) et contenaient de fausses affirmations, des rumeurs et des conjectures sur l'évolution de la situation relative au COVID-19. Certaines autorités chargées de l'application de la loi qui ont participé à l'enquête ont indiqué que, dans leur pays, la mésinformation était liée au commerce illicite de produits médicaux frauduleux.

Certains pays membres ont constaté avec préoccupation que la mésinformation propageait, au sein de la population, une panique et un désordre social déjà exacerbés par la pandémie. Les autorités chargées de l'application de la loi ont signalé des cas de fausses informations diffusées en ligne au sujet du nombre de personnes infectées et de l'apparition du virus dans des zones non touchées.

[10] OMS, informations consultées et extraites le 21 mai 2020 à l'adresse https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf

[11] Reuters Institute, informations consultées et extraites le 22 mai 2020 à l'adresse https://reutersinstitute.politics.ox.ac.uk/research

D'autres affaires de mésinformation impliquaient des escroqueries par l'intermédiaire de SMS contenant des offres « trop belles pour être vraies », telles que des produits alimentaires gratuits, des aides spéciales ou d'importantes remises dans des supermarchés. Les services chargés de l'application de la loi estiment que la plupart de ces messages ont été diffusés dans la population dans le but de provoquer d'importants rassemblements et d'en tirer parti.

Fig. 3 : Avertissement publié par l'OMS informant le public de la circulation d'une fausse nouvelle sur le COVID-19 via WhatsApp[12]

LA RÉPONSE D'INTERPOL

Face à une cybercriminalité en rapide évolution durant la pandémie de COVID-19, INTERPOL élabore et conduit la réponse mondiale des services chargés de l'application de la loi aux cybermenaces associées. Sa Direction de la Cybercriminalité collabore dans plusieurs domaines avec les pays membres, les partenaires du secteur privé et les communautés d'experts en matière de cybersécurité du monde entier.

Afin d'aider les pays membres à prévenir et à combattre la cybercriminalité durant la pandémie, les actions suivantes ont été ou sont encore menées par INTERPOL :

- Organisation de réunions de crise virtuelles avec diverses parties prenantes afin de proposer aux pays membres des services adaptés en vue de prévenir et de détecter les cyberinfractions liées au COVID-19 et d'enquêter à leur sujet. Il s'agit notamment de réunions stratégiques des chefs des unités nationales et régionales de lutte contre la cybercriminalité et du Groupe d'experts mondial d'INTERPOL sur la cybercriminalité[13].

[12] OMS, informations consultées et extraites le 21 mai 2020 à l'adresse https://www.who.int/india/emergencies/coronavirus-disease-(covid-19)/fake-news-alert

[13] Le Groupe d'experts mondial d'INTERPOL sur la cybercriminalité est un réseau de spécialistes de la cybercriminalité des pays membres, des secteurs privé et public et du monde universitaire qui mettent en commun informations et bonnes pratiques et conseillent le Secrétariat général d'INTERPOL dans le cadre de l'élaboration des politiques et de la mise en œuvre des projets en matière de cybercriminalité.

- INTERPOL participe également de manière active aux discussions stratégiques multilatérales menées par le Forum économique mondial[14] en vue de constituer des partenariats et une alliance contre la cybercriminalité. Il est également membre du Conseil consultatif du Centre pour la cybersécurité du Forum économique mondial.
- **Publication de notices mauves INTERPOL**[15] afin d'informer la communauté des services chargés de l'application de la loi des cybermenaces nouvelles et présentant un risque élevé. Ces alertes mondiales, envoyées par l'intermédiaire du réseau sécurisé de l'Organisation, portent notamment sur les menaces suivantes[16] :
  - **Les attaques par rançongiciel contre des infrastructures essentielles et des hôpitaux :** le CFC d'INTERPOL a détecté des tentatives de compromission et d'exécution de rançongiciels ciblant des organisations et des infrastructures clés jouant un rôle essentiel face au COVID-19 ;
  - **Utilisation et diffusion d'un cheval de Troie bancaire :** un cheval de Troie bancaire a exploité la vulnérabilité d'un service national afin de se faire passer pour l'entité en question et d'envoyer des SMS incitant à télécharger un contenu lié au COVID-19 et comportant un lien malveillant ;
  - **Envoi de périphériques USB malveillants :** le CFC a recueilli des informations sur le nouveau vecteur d'attaque d'un groupe de cybercriminels, à savoir l'envoi par courrier de périphériques USB malveillants dans le cadre de « cadeaux » afin d'accéder aux réseaux d'entreprises et de dérober des informations sensibles ;
  - **Utilisation et diffusion d'un logiciel malveillant (cheval de Troie) :** ce logiciel malveillant appelé « Coronavirus » rend les disques inutilisables par écrasement de l'enregistrement d'amorçage maître.
- Réunion d'un **Groupe spécial mondial sur les domaines malveillants.** Constitué d'officiers de renseignement en matière de cybercriminalité, d'experts de partenaires du secteur privé et de professionnels des services nationaux chargés de l'application de la loi, ce groupe spécial a pour objectif d'identifier et de cibler les acteurs de la menace et les infrastructures communes liés aux domaines malveillants afin de désorganiser ce type de menace et de l'atténuer.

  En juin 2020, le Groupe spécial avait repéré et analysé environ 200 000 domaines malveillants. S'appuyant sur ces éléments, la Direction de la Cybercriminalité a diffusé des signalements d'activités cybercriminelles contenant des données utiles auprès de plus de 80 pays membres concernés.
  - Réalisation d'une **campagne de sensibilisation mondiale portant sur les cybermenaces liées au COVID19, #WashYourCyberHands**, lancée en mai 2020

[14] Forum économique mondial, informations consultées et extraites le 14 juillet 2020 à l'adresse https://www.weforum.org/agenda/2019/11/why-public-private-partnerships-are-critical-for-global-cybersecurity/ ; https://www.weforum.org/agenda/2020/01/partnerships-are-our-best-weapon-in-the-fight-against-cybercrime-heres-why/

[15] INTERPOL publie des notices mauves à l'intention des pays membres pour solliciter ou fournir des informations sur des modes opératoires, des objets, des dispositifs et des méthodes de dissimulation employés par des malfaiteurs.

[16] Le détail des notices mauves a été omis afin de ne pas compromettre les opérations de lutte contre la cybercriminalité actuellement menées par INTERPOL.

avec les pays membres et 23 partenaires extérieurs afin de mettre en garde le public contre les grandes cybermenaces en lien avec la pandémie de coronavirus et de promouvoir les principes d'une bonne « hygiène » en ligne. Ayant pour but de protéger les populations des cybermalfaiteurs qui cherchent à tirer parti de la flambée de COVID-19 pour voler des données, provoquer des perturbations ou commettre des escroqueries, cette campagne a appuyé les efforts de prévention déployés par les services nationaux chargés de l'application de la loi contre l'augmentation des cybermenaces dans ce contexte. Conçus par INTERPOL et ses partenaires, les visuels de la campagne et les publications sur les médias sociaux ont touché une audience de quelque 7,5 millions de personnes sur Internet. Pour le seul Twitter (@INTERPOL_Cyber), le mot dièse #WashYourCyberHands a été repris environ 10 000 fois.

PRIORITÉS ET RECOMMANDATIONS

Pour faire en sorte que l'appui et les services fournis par INTERPOL à ses pays membres demeurent aussi efficaces que possible s'agissant d'atténuer les cybermenaces liées au COVID-19, nous avons recensé les priorités et recommandations ci-dessous :

- **Permettre un échange d'informations en temps opportun.** Des informations récentes sur les cyberattaques qui viennent d'être détectées permettent à la Direction de la Cybercriminalité de prévoir avec précision les nouvelles tendances et de partager les informations sur les modes opératoires des malfaiteurs par l'intermédiaire du réseau mondial d'INTERPOL afin d'encourager la vigilance et la prévention en matière de cybercriminalité. Cela vaut en particulier pour les attaques par rançongiciel contre les gouvernements, les infrastructures essentielles et le secteur de la santé, qui sont susceptibles de constituer un risque et un danger majeurs pour la santé et la sécurité publiques. Le fait de recevoir rapidement des informations utiles permet à INTERPOL d'aider les pays membres à élaborer et à mettre en place une riposte efficace.

- **Améliorer la collaboration et la coopération entre les polices des pays membres.** Compte tenu de l'évolution des cybermenaces transnationales du fait du COVID-19, INTERPOL attire l'attention sur l'importance d'une collaboration entre les autorités nationales chargées de l'application de la loi, et d'une réponse dans les meilleurs délais aux demandes d'informations que leur adressent les autres pays. La coopération et l'échange d'informations sont particulièrement décisifs face aux cybermenaces suivantes :

  - Attaques par rançongiciel contre des infrastructures essentielles, indicateur de compromission, adresses bitcoin ;
  - Affaires liées aux escroqueries par paiement anticipé et aux escroqueries aux faux ordres de virement ;
  - Diffusion de logiciels malveillants au moyen d'applications non gouvernementales de recherche des contacts ;
  - Informations au sujet de campagnes faisant appel à de nombreux domaines malveillants.

- **Utiliser la Plateforme collaborative d'INTERPOL sur la cybercriminalité**[17]**.** Conçue pour permettre les échanges de connaissances et la coordination opérationnelle, cette plateforme offre aux pays membres une solution sécurisée pour participer à des cellules spéciales communes réunissant plusieurs parties prenantes et plusieurs pays aux fins de la lutte contre la criminalité ciblant les systèmes informatiques. Elle permet ainsi une communication directe entre les équipes opérationnelles des pays membres et avec INTERPOL, d'où un partage efficace des informations en matière de cybercriminalité en vue d'élaborer une riposte opérationnelle rapide aux perturbations constatées.

- **Mettre en œuvre des mesures de prévention et de sensibilisation.** Dans le monde entier, l'évolution des cybermenaces liées au COVID-19 devrait continuer à présenter des difficultés d'ordre juridique et opérationnel aux services chargés de l'application de la loi. Pour les atténuer, il est essentiel de mener une action de prévention en éduquant le public et en lui donnant les moyens d'assurer sa sécurité sur Internet. Les pays membres sont encouragés à diffuser les principaux messages de la campagne mondiale #WashYourCyberHands d'INTERPOL au sein de leur population, par l'intermédiaire des plateformes de médias sociaux, et à lancer des campagnes de sensibilisation semblables au niveau national.

- **Améliorer les capacités d'enquête en matière de cybercriminalité.** Alors que les cybermenaces continuent à évoluer, en relation directe ou non avec la pandémie, il est particulièrement important que les services chargés de l'application de la loi soient dotés de technologies et de capacités spécialisées. Conscient de l'importance de renforcer les compétences de ses pays membres durant la crise mondiale, INTERPOL a lancé son **Académie mondiale virtuelle** qui a pour objet d'offrir toute une palette de formations en ligne aux services chargés de l'application de la loi. La Direction de la Cybercriminalité de l'Organisation propose en ligne des formations et des webinaires destinés à améliorer les capacités des pays membres à répondre aux nouvelles cybermenaces et à enquêter avec succès sur les cyberinfractions durant la crise mondiale et au-delà.

- **Renforcer les partenariats public-privé.** Depuis le début de la pandémie de COVID-19, ces partenariats ont grandement contribué à atténuer les nouvelles cybermenaces. En partageant leurs renseignements et leur expertise concernant les tendances récentes et en fournissant une assistance technique, les entreprises du secteur privé peuvent être des partenaires précieux pour les services chargés de l'application de la loi.

  À cet égard, depuis janvier 2020, la Direction de la Cybercriminalité d'INTERPOL a rassemblé les données et informations sur les cybermenaces liées au COVID-19 communiquées par les pays membres, les partenaires privés de l'Organisation, les Cellules nationales de réponse aux attaques informatiques (CERT) et la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN), ainsi que par les groupes de partage d'informations en ligne tels que Slack. La diversité de ces partenaires a enrichi l'ensemble de données et apporté la preuve de son utilité s'agissant de fournir rapidement aux pays membres l'assistance requise. Mesurant

[17] La Plateforme collaborative d'INTERPOL sur la cybercriminalité est hébergée au sein du Pôle de la cybercriminalité de la Plateforme de connaissances mondiale d'INTERPOL qui repose sur la technologie de Plateforme collaborative sécurisée.

le caractère positif de ces collaborations, INTERPOL s'est donné pour objectif de développer une base de données à laquelle toutes les parties prenantes pourront accéder et contribuer afin d'élaborer la réponse la plus efficace possible aux menaces de la cybercriminalité.

Fondamentalement, l'instauration de relations solides entre les services chargés de l'application de la loi et le secteur privé suscite un sentiment de responsabilité partagée dans la lutte contre les cybermenaces liées au COVID-19 et permet d'apporter une réponse ciblée et rapide à celles qui surgissent.

- **Élaborer et mettre en œuvre des stratégies nationales de lutte contre la cybercriminalité.** L'enquête réalisée récemment par INTERPOL a mis en évidence l'absence, dans 30 pays membres, de stratégie nationale de lutte contre la cybercriminalité en réponse à la pandémie de COVID-19. Ce constat souligne la nécessité de mettre en place une telle stratégie afin de renforcer la résilience des infrastructures et services nationaux, ce qui peut aider les pays à combattre efficacement les cybermenaces et à protéger les populations contre les violations de données durant la crise mondiale et au-delà.

PRÉVISIONS À COURT TERME

L'analyse des informations communiquées par les services chargés de l'application de la loi et les entités du secteur privé indique que la détérioration du paysage de la cybermenace devrait se poursuivre. Les prévisions ci-dessous de la Direction de la Cybercriminalité d'INTERPOL mettent en évidence les principaux domaines qui constitueront vraisemblablement une source de préoccupation :

- Alors que le COVID-19 est toujours présent dans le monde, il y a tout lieu de penser que l'on enregistrera prochainement une nouvelle hausse de la cybercriminalité. Attirés par les vulnérabilités liées au télétravail et la possibilité d'augmenter leurs gains, les cybermalfaiteurs vont très probablement intensifier leurs activités et perfectionner leurs modes opératoires ;
- Les vulnérabilités liées aux politiques de télétravail continueront sans doute à être exploitées par les cybermalfaiteurs qui cherchent à obtenir les données d'identification d'employés au moyen d'outils et de logiciels bureautiques essentiels. Les données à caractère personnel dérobées peuvent également être utilisées dans le cadre de nouvelles cyberattaques ;
- Poussant les malfaiteurs à trouver d'autres sources de revenus, les conséquences des mesures de confinement liées au coronavirus sur les autres domaines de criminalité contribuent également au développement de la cybercriminalité. Il est donc probable que certains malfaiteurs utiliseront les cryptomarchés pour proposer de la « cybercriminalité en tant que service », facilitant ainsi l'accès à ce type de criminalité ;
- Tirant parti de la panique générée par la pandémie, les acteurs de la menace continueront sans doute à se livrer à des escroqueries en ligne et à des campagnes d'hameçonnage ayant pour thème le coronavirus. Les escroqueries aux faux ordres

de virement vont probablement connaître elles aussi une croissance importante en raison du ralentissement de l'activité économique et de l'évolution du monde de l'entreprise, offrant ainsi de nouvelles possibilités en matière d'activités criminelles ;

- Par ailleurs, lorsque des vaccins ou des médicaments contre le COVID-19 seront disponibles, il est fort probable que l'on enregistrera une nouvelle hausse de l'hameçonnage en lien avec ces produits médicaux, ainsi que des intrusions dans les réseaux et des cyberattaques visant à voler des données ;
- Les attaques par rançongiciel ciblant le secteur de la santé et les chaînes logistiques associées risquent de se poursuivre à un rythme plus soutenu, favorisé par la diversification des vecteurs d'attaque ;
- On s'attend à ce que les acteurs de la menace ciblent les données à caractère personnel des particuliers en usurpant l'identité des fournisseurs de contenus numériques et en exploitant ces derniers ;
- Même lorsque le nombre de cas de coronavirus aura diminué, les cybermalfaiteurs adapteront très certainement leurs escroqueries pour tirer parti de la situation qui fera suite à la pandémie et exploiter le plus possible de victimes.

CONCLUSION

Les cybermalfaiteurs, qui exploitent la peur et l'incertitude liées à l'instabilité de la situation sociale et économique dans le monde, préparent et multiplient leurs attaques à un rythme très préoccupant. En parallèle, la dépendance accrue à la connectivité et aux infrastructures numériques du fait du confinement mondial a renforcé les possibilités d'intrusion et d'attaque informatiques.

Malgré ces perspectives, INTERPOL agit de manière proactive et prend toutes les mesures appropriées pour aider ses pays membres plongés dans une crise sans précédent. L'Organisation se prépare également aux menaces de l'après-COVID19. La pandémie offre une occasion exceptionnelle de réfléchir aux capacités actuelles et aux moyens de les améliorer en vue d'une meilleure préparation et d'une résilience accrue aux éventuels chocs à venir.

Enfin, cette pandémie mondiale a montré à quel point il était important d'apporter une réponse internationale fondée sur la collaboration et la coordination. La priorité numéro un s'agissant de faire face à l'augmentation de ces cybermenaces est de renforcer encore la coopération policière internationale dans le cadre des activités opérationnelles et d'améliorer l'échange d'informations sur la cybercriminalité avec divers partenaires de l'écosystème mondial de la cybersécurité.

Faisant porter ses efforts sur les grands piliers de son action – la réponse aux cybermenaces, les cyberopérations et le renforcement des capacités de lutte contre la cybercriminalité –, la Direction de la Cybercriminalité d'INTERPOL continuera de s'employer à atténuer les conséquences de la cybercriminalité dans le monde et à protéger les populations en leur garantissant un monde plus sûr.

INTERPOL

À PROPOS D'INTERPOL

INTERPOL is the world's largest international police organization. Our role is to assist law enforcement agencies in our 194 member countries to combat all forms of transnational crime. We work to help police across the world meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. Our services include targeted training, expert investigative support, specialized databases and secure police communications channels.

NOTRE VISION :
« RELIER LES POLICES POUR UN MONDE PLUS SÛR »

Notre vision est celle d'un monde dans lequel chaque professionnel des services chargés de l'application de la loi pourra, par la voie d'INTERPOL, transmettre, partager et consulter en toute sécurité des informations de police vitales, à tout moment et en tout lieu où il en aura besoin, afin d'assurer la sécurité des personnes sur toute la surface du globe. Nous apportons et travaillons à offrir continuellement des solutions innovantes et de pointe aux problèmes qui se posent à l'échelle mondiale en matière de police et de sécurité.