INTERPOL

ÉVALUATION 2021 DES CYBERMENACES EN AFRIQUE

PRINCIPALES OBSERVATIONS D'INTERPOL SUR LA CYBERCRIMINALITE EN AFRIQUE

Octobre 2021

TABLE DES MATIÈRES

AVANT-PROPOS

La portée de la cybercriminalité dépasse les cadres nationaux. Conjuguée à la dépendance accrue aux activités en ligne au cours de la pandémie de COVID-19, elle représente un redoutable enjeu de sécurité dans le monde entier. Cette situation est exacerbée par la « carence » en cybercapacités des services chargés de l'application de la loi au sein des différentes régions et entre celles-ci. Cette carence est un facteur clé de facilitation des opportunités, des infrastructures et des réseaux criminels.

Consciente de cet enjeu, INTERPOL apporte un appui à ses 194 pays membres en les accompagnant dans le renforcement de leurs capacités en matière d'application de la loi et de leurs moyens de lutte contre la cybercriminalité. L'Organisation propose un éventail d'outils, de plateformes et un appui opérationnel afin de connecter les services de police et de créer un monde plus sûr. En particulier, son Programme mondial de lutte contre la cybercriminalité a joué un rôle crucial dans le pilotage de la réponse apportée à cette menace par la communauté mondiale des services chargés de l'application de la loi.

Le partenariat est au cœur de ces efforts. La collaboration avec les différents acteurs de l'écosystème mondial de la cybersécurité est indispensable. En effet, la richesse de leurs points de vue, de leur expertise et de leurs ensembles de données contribue à l'élaboration de politiques et de réponses opérationnelles efficaces à opposer à la cybercriminalité. Les partenariats nous permettent aussi de mutualiser nos connaissances afin de pouvoir faire preuve de résilience et d'agilité en période d'incertitude.

S'appuyant sur ce cadre de partenariat, INTERPOL adopte une approche de coordination opérationnelle régionalisée pour lutter contre la cybercriminalité. En effet, bien qu'il s'agisse d'un enjeu mondial, chaque région y répond différemment. Et pour vaincre les menaces plus efficacement, nous devons en comprendre les évolutions et les préjudices qu'elles provoquent dans chaque région.

Partant de ce constat, INTERPOL a préparé ce rapport d'évaluation des cybermenaces en Afrique au bénéfice de ses pays membres dans la région. Son objectif est de dresser un panorama précis des menaces afin de pouvoir apporter un appui sur mesure. Ce rapport a été préparé sous l'égide de l'AFJOC (Desk africain pour les opérations conjointes de lutte contre la cybercriminalité) avec le soutien du Bureau britannique des Affaires étrangères, du Commonwealth et du Développement.

À partir de cette évaluation des menaces, le Desk africain pour les opérations conjointes de lutte contre la cybercriminalité, nouvellement créé au titre du projet AFJOC, va pouvoir piloter des actions coordonnées, fondées sur le renseignement pour lutter contre la cybercriminalité et ses auteurs dans les pays membres africains. Pour appuyer efficacement la région, INTERPOL travaille également étroitement avec les organisations régionales clés comme l'Union africaine et AFRIPOL pour maximiser les efforts de coordination et de mise en œuvre et dynamiser les capacités et les moyens de lutte régionaux contre la cybercriminalité.

Je ne doute pas que ce rapport contribue à remédier aux carences constatées au sein de la région africaine et au-delà et qu'il contribue à l'efficacité de la réponse de la communauté mondiale des services chargés de l'application de la loi. Nous remercions les pays membres africains et nos partenaires pour leur solide engagement dans cette entreprise.

Stephen Kavanagh
Directeur exécutif des services policiers
INTERPOL

AVANT-PROPOS

Le continent africain offre un potentiel exceptionnel en matière de technologies de l'information et de la communication en raison notamment de sa jeunesse. En effet, en 2020, près de 60 % de la population africaine avaient moins de 25 ans. Ce facteur génère une forte croissance dans l'utilisation des nouvelles technologies.

Toutefois, nous assistons également au regain des activités liées à la cybercriminalité, en particulier en cette période de pandémie de COVID-19. Les destructions d'emplois dues à la pandémie et l'anémie de la croissance économique ont ouvert la voie à de nouvelles opportunités pour les organisations criminelles. Cela explique l'attention particulière que la Commission de l'Union africaine accorde à la lutte contre toutes les formes de criminalité organisée : blanchiment d'argent, criminalité transnationale et cybercriminalité.

En ce qui concerne la couverture Internet et la bande passante, l'Afrique reste mal desservie, en particulier dans les zones rurales, alors que ses réseaux de téléphonie et Internet affichent la croissance la plus rapide au monde. Sur ce continent jeune, chaque défi économique est relevé par une solution innovante qui, malheureusement, frôle parfois les limites de la légalité. Ainsi, le faible nombre d'installations bancaires à la disposition des populations africaines a favorisé l'émergence de nouveaux services financiers comme la banque mobile, mais aussi la résurgence de nouvelles formes d'escroquerie liées à ces nouvelles technologies.

Notre stratégie pour lutter contre la cybercriminalité repose sur trois piliers :

- Mieux sensibiliser les populations
- Renforcer les dispositions des politiques, des traités et des lois ordinaires pour lutter contre les cybermalfaiteurs
- Déployer des technologies à l'échelle nationale pour renforcer la défense cyber

En collaboration avec INTERPOL, AFRIPOL a commencé à former les officiers des polices nationales à la protection contre les attaques DNS (serveur de noms de domaine). Une stratégie de rapprochement public-privé a aussi été mise en place pour conclure des partenariats avec des leaders d'Internet et des fournisseurs de cybermonnaies.

Internet a aboli les frontières. Une cyberattaque lancée en Afrique peut avoir des conséquences directes ou indirectes sur n'importe quelle citoyenne ou quel citoyen du monde. Cette lutte est une lutte de longue haleine et nous devons être unis si nous voulons vaincre efficacement la cybercriminalité en Afrique et dans le monde.

Tarek A. Sharif
Directeur exécutif
AFRIPOL

ABRÉVIATIONS ET ACRONYMES

AFJOC	Desk africain pour les opérations conjointes de lutte contre la cybercriminalité
FOVI	Escroquerie aux faux ordres de virement
AC	Autorité de certification
CCP	Programme international de contrôle des conteneurs
CD	Direction de la Cybercriminalité
CNP	Fraude au paiement à distance
CKE	Échange de connaissances sur la cybercriminalité
ACS	Autorité de cybersécurité
CTR	Unité Réponse aux cybermenaces
DDoS	Déni de service distribué
FCDO	Bureau des Affaires étrangères, du Commonwealth et du Développement
FCU	Unité Criminalité financière
Gbps	Gigabits par seconde
ISPA	Programme INTERPOL d'appui à l'Union africaine
IES	Institut d'études de sécurité
LEA	Services chargés de l'application de la loi
M.O.	Mode opératoire
NPF	Police nigériane
GCO	Groupe criminel organisé
DCP	Donnée à caractère personnel
RAT	Cheval de Troie d'accès à distance
SABRIC	South African Banking Risk Information Centre
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
TTP	Tactiques, techniques et procédures
VPS	Serveur privé virtuel
VSA	Administrateur de système/serveur virtuel

REMERCIEMENTS

Le Rapport 2021 d'évaluation des cybermenaces en Afrique a été préparé par la Direction de la Cybercriminalité d'INTERPOL sous l'égide de l'AFJOC (Desk africain pour les opérations conjointes de lutte contre la cybercriminalité) et avec le financement du Bureau britannique des Affaires étrangères, du Commonwealth et du Développement (FCDO). Le programme INTERPOL d'appui à l'Union africaine (ISPA) y a également contribué, avec le soutien du ministère fédéral des Affaires étrangères de l'Allemagne. Ce rapport a bénéficié des données et de l'expertise de partenaires privés d'INTERPOL, à savoir Group-IB, Kaspersky, Palo Alto Networks et Trend Micro.

RÉSUMÉ

Ce rapport fait la somme des observations recueillies par INTERPOL sur les principales cybermenaces qui affectent la région africaine. Il offre aussi une analyse approfondie de leur impact ainsi que des exemples de l'appui opérationnel apporté par l'Organisation pour lutter contre la cybercriminalité et en présente la stratégie régionale de lutte contre la cybercriminalité déployée pour l'Afrique. Sur la base des retours des pays membres africains d'INTERPOL et des données recueillies auprès de ses partenaires privés, les menaces les plus prééminentes sont les suivantes :

- **Escroqueries en ligne** – Pour les pays membres africains, les escroqueries en ligne représentent la cybermenace la plus fréquemment signalée et la plus pressante dans la région. Cette menace cible et exploite les peurs, les insécurités et les vulnérabilités des victimes en recourant au hameçonnage, aux campagnes d'envoi massif de messages électroniques et à l'ingénierie sociale. Les pays membres ont signalé une hausse accentuée du nombre d'escroqueries bancaires en ligne, et notamment de cas de fraude bancaire et de fraude à la carte de crédit.
- **Extorsion en ligne** – Cette menace a aussi été identifiée comme l'une des cybermenaces majeures dans la région. L'extorsion en ligne cible les particuliers soit en alléguant de la détention d'images sexuellement compromettantes, soit par des campagnes de chantage direct. Même si ces menaces sont loin d'être nouvelles, la transformation numérique de la société – en particulier au sein de la région africaine – a créé de nouveaux vecteurs d'attaque pour les malfaiteurs pour à la fois brouiller leur identité et cibler de nouvelles victimes.
- **Escroqueries aux faux ordres de virement** – Aux côtés des escroqueries en ligne, les escroqueries aux faux ordres de virement (FOVI) ont été identifiées comme une préoccupation et une menace de premier plan pour la région. En Afrique, les entreprises et les organisations qui dépendent lourdement des transactions par virement sont vulnérables à cette menace. De plus, la pandémie de COVID-19 a favorisé cette forme de cybercriminalité.
- **Rançongiciels** – La menace des rançongiciels se répand sur le continent africain. Au cours de la seule année 2020, plus de 61 % des entreprises de la région auraient subi des attaques par rançongiciel.[1] Ces attaques ont ciblé les infrastructures essentielles de certains pays africains, notamment dans le secteur de la santé et le secteur maritime.[2]
- **Botnets** – Les botnets sont des réseaux de machines infectées utilisées pour automatiser des campagnes à grande échelle comme des attaques par déni de service distribué (DDoS), des campagnes d'hameçonnage, la propagation de maliciels, etc. Près de 50 000 détections de victimes de botnets ont été dénombrées en Afrique, avec une moyenne mensuelle de 3 900 détections. Au cours des cinq dernières années, l'Afrique a connu de nombreux cas médiatisés d'attaques DDoS contre des infrastructures essentielles.

Prenant acte de la nécessité de faire évoluer la lutte contre la cybercriminalité au sein de l'Afrique en tant que région embrassant la transformation numérique, le rapport présente en conclusion la stratégie régionale d'INTERPOL pour lutter contre la cybercriminalité et appuyer ses pays membres africains. Cette stratégie englobe les quatre objectifs stratégiques suivants :

- **renforcer le renseignement sur la cybercriminalité afin d'y apporter des réponses efficaces** ;
- **renforcer la coopération pour les opérations conjointes menées contre la cybercriminalité ;**
- **développer les capacités et les moyens régionaux de lutte contre la cybercriminalité ;**
- **promouvoir une bonne cyberhygiène afin de rendre le cyberespace plus sûr.**

INTERPOL se tient prête pour appuyer ses pays membres africains dans la réalisation de ces objectifs et pour poursuivre le développement d'un cadre opérationnel conjoint en vue de renforcer les actions coordonnées de lutte contre la cybercriminalité menées en Afrique. Les efforts collectifs déployés pour échanger les renseignements et formuler un cadre opérationnel conjoint dynamiseront les capacités et les moyens régionaux de lutte contre la cybercriminalité.

---

1 Lumu, *2020 Ransomware Flashcard*, consultable à l'adresse : [https://lumu.io/resources/2020-ransomware-flashcard/]

2 Institut d'études de sécurité, *Africa can't risk a major maritime cyber attack*. Reva, D., 28 octobre 2020. Consultable à l'adresse : [https://issafrica.org/iss-today/africa-cant-risk-a-major-maritime-cyber-attack]

1. INTRODUCTION

L'Afrique compte plus de 500 millions d'internautes, devançant à ce titre d'autres régions comme l'Amérique du Nord, l'Amérique du Sud et le Moyen-Orient.[3] Ce nombre d'utilisateurs représente près de 38 % de la population régionale et devrait donc continuer à augmenter au cours des prochaines années en raison de la digitalisation accélérée de la société. Les pays de tête sont le Kenya, dont 83 % de la population sont en ligne, le Nigéria avec 60 % et l'Afrique du Sud avec 56 %.[3] La banque mobile en particulier est largement utilisée dans ces trois pays, contribuant au rôle actif de l'Afrique dans les services financiers en ligne.[4] Cette situation induit une menace future non négligeable, avec la montée en puissance des applications malveillantes exploitant les vulnérabilités croissantes des appareils mobiles.

En 2021, 38 % des citoyens africains sont en ligne

En dépit de la forte demande pour la banque mobile, la fracture numérique reste problématique, en particulier alors que les pays membres africains accélèrent l'intégration des infrastructures numériques aux fondations de leur société, notamment aux infrastructures publiques, bancaires, commerciales et essentielles. Cette transformation souligne le besoin urgent de disposer de paramètres et de standards de cybersécurité en adéquation avec les demandes et les besoins futurs de cette communauté, notamment l'inclusion financière.[5]

Toutefois, l'absence de tels standards est un fait généralisé en Afrique. 90 % des entreprises africaines n'utilisent pas les protocoles de cybersécurité nécessaires.[6] Sans ces derniers, les acteurs des menaces exploitent sans peine les vulnérabilités croissantes en inventant de nouveaux vecteurs de cyberattaques. Ce qui se traduit par des pertes financières massives. En 2016, la cybercriminalité a coûté 36 millions USD à l'économie kényane, 573 millions USD à l'économie sud-africaine et 500 millions USD à l'économie nigériane.[7] Selon une étude réalisée par Deloitte, les pertes des institutions financières au Kenya, au Rwanda, en Ouganda, en Tanzanie et en Zambie depuis 2011 s'élèvent à plus de 245 millions USD.

> ***« Plus de 90 % des entreprises africaines n'utilisent pas les protocoles de cybersécurité nécessaires. »***

Source : CGTN

---

[3] *Council on Foreign Relations, Last Month, Over Half-a-Billion Africans Accessed the Internet*, Campbell, juillet 2019. Consultable à l'adresse : [https://www.cfr.org/blog/last-month-over-half-billion-Africans-accessed-internet]

[4] *Cision, Africa Leads World in Digital Financial Services Deployments with Prepaid Cards an Important Part of Mix, Says Axiom Prepaid Holdings Reps*, juin 2020. Consultable à l'adresse : [https://www.prweb.com/releases/Africa_leads_world_in_digital_financial_services_deployments_with_prepaid_cards_an_important_part_of_mix_says_axiom_prepaid_holdings_reps/prweb17214821.htm]

[5] Société financière internationale, *Digital Access: The Future of Financial Inclusion in Africa*, 2018. Consultable à l'adresse : [https://www.ifc.org/wps/wcm/connect/region__ext_content/ifc_external_corporate_site/sub-saharan+africa/resources/201805_report_digital-access-africa]

[6] CGTN, *Rights group launches tool to stem cybercrime in Africa*, Odonkor, A, 27 octobre 2020. Consultable à l'adresse : [https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html]

[7] *SciDev.Net, Cybercrime in Africa: Facts and figures*. Fassassi, Akoussan juillet, 2016. Consultable à l'adresse : [https://www.scidev.net/sub-saharan-africa/features/cybercrime-africa-facts-figures/]

Au cours de l'année écoulée, la pandémie de COVID-19 a accéléré la croissance de l'écosystème de la cybercriminalité,[8] avec une fracture numérique persistante et des vulnérabilités de cybersécurité croissantes dans toute la région. À l'instar d'autres régions, l'Afrique a fait l'objet d'attaques visant ses infrastructures essentielles et ses services de première ligne au cours de la pandémie. Ce phénomène a été particulièrement marqué en Afrique du Sud et au Botswana. Ainsi, en Afrique du Sud, Life Healthcare Group, une organisation qui gère 66 établissements de santé, a été victime d'une cyberattaque grave et durable.[9]

Et, de fait, la transformation numérique accrue de l'Afrique facilite l'émergence de nouveaux vecteurs d'attaque et de nouvelles opportunités pour les cybermalfaiteurs. Prenant acte de l'ampleur du problème causé par les cybermenaces dans la région, nous présentons dans la section suivante de ce rapport une analyse approfondie du panorama africain des cybermenaces.

Une étude réalisée par l'entreprise de cybersécurité kényane Serianu a montré que la cybercriminalité a amputé le PIB africain de plus de 10 % en 2021, avec un coût estimé à 4,12 milliards USD.[10] Trend Micro, un partenaire d'INTERPOL, a enregistré des millions de détections de menaces en Afrique entre janvier 2020 et février 2021 :

- Courriels : 679 millions de détections
- Fichiers : 8,2 millions de détections
- Web : 14,3 millions de détections

Plus spécifiquement, l'Afrique du Sud a enregistré au total 230 millions de détections de menaces, le Kenya 72 millions et le Maroc 71 millions. En Afrique du Sud, 219 millions de détections ont concerné des menaces liées aux courriels. Ce pays a également affiché le taux le plus élevé de tentatives ciblées de rançongiciels et d'escroqueries aux FOVI.

[8] *Symantec, Cybercrime & Cyber Security Trends in Africa*. Novembre 2016. Consultable à l'adresse : [https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf]

[9] *Cybercrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, Morgan, S., 13 novembre 2020. Consultable à l'adresse : [https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/]

[10] *Physorg, Rights group launches tool to stem cybercrime in Africa*. Consultable à l'adresse : [https://phys.org/news/2021-05-rights-group-tool-stem-cybercrime.html]

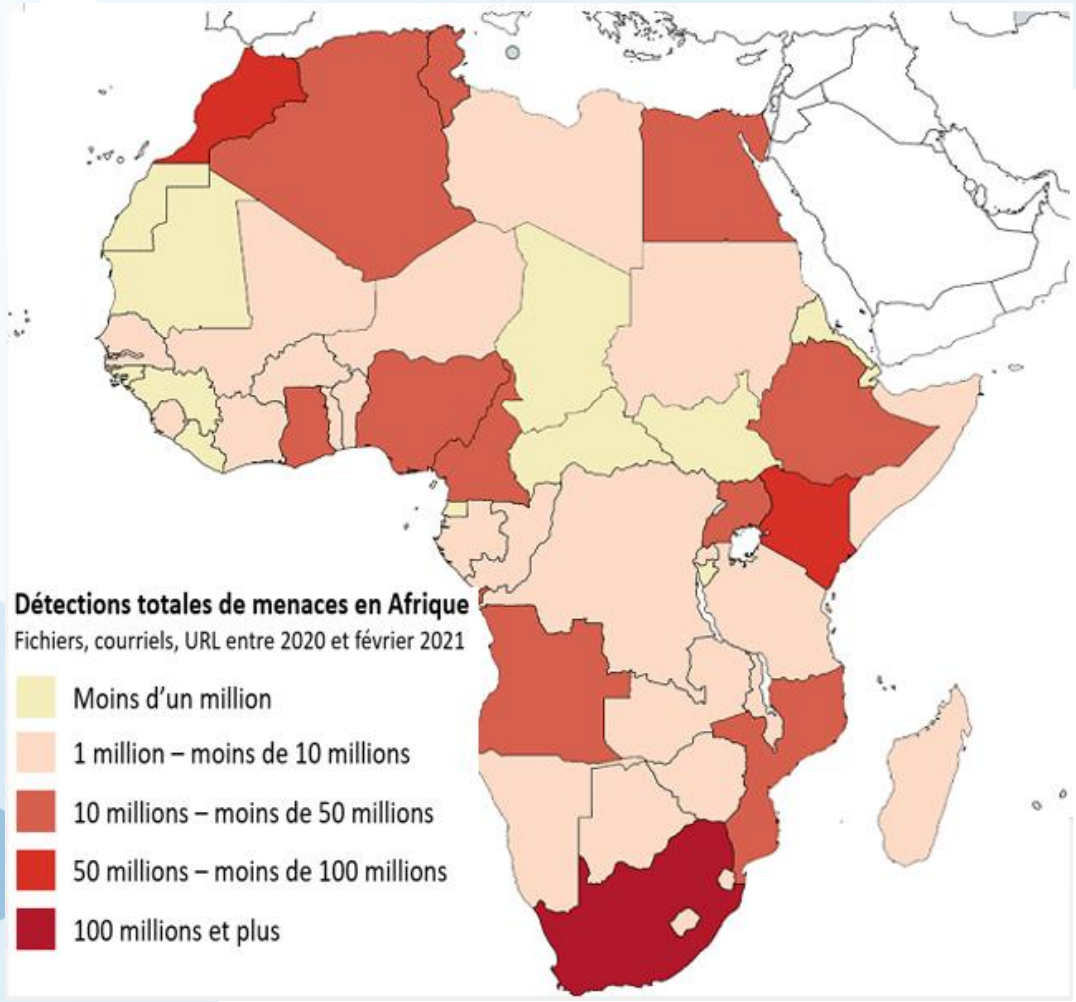


Figure 1. Détection globale des cybermenaces en Afrique à l'aide des capteurs de Trend Micro (Source : Trend Micro)

L'exploitation de ces vulnérabilités en Afrique du Sud a été confirmée par Accenture, qui a placé le pays au troisième rang mondial des victimes de la cybercriminalité pour un coût annuel de 2,2 milliards de rands sud-africains.[11] L'ampleur de cette forme de cybercriminalité est corroborée par l'augmentation de 100 % de la fraude aux applications bancaires dans le pays qui subit 577 attaques de maliciels par heure.[12] Ces attaques de maliciels sont l'une des nouvelles menaces.

En raison de la diversification et de l'évolution des vecteurs d'attaque ainsi que de la stratégie ciblée contre les organisations chargées de la réponse de première ligne, les chaînes d'approvisionnement mondiales et les infrastructures essentielles, il n'a jamais été aussi urgent, d'une part, de trouver une voie de sortie et, d'autre part, de concentrer les efforts sur le renforcement de la sécurité et de la sûreté dans le cyberespace pour tous les pays membres africains.

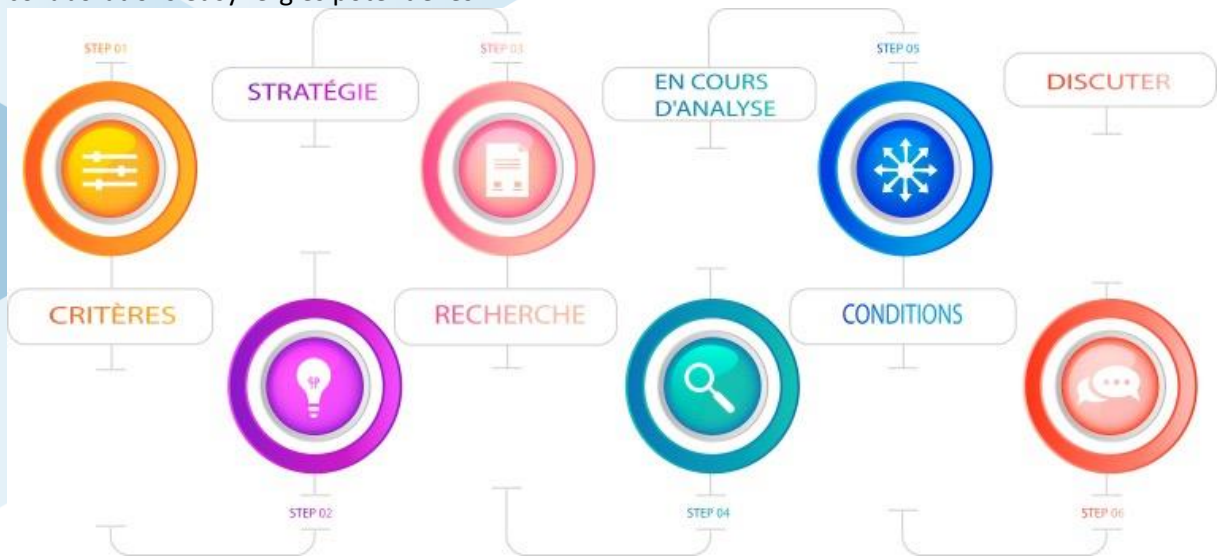
[11] *Accenture, Insight into the cyber threat landscape in South Africa*, 27 mai 2020. Consultable à l'adresse : [https://www.accenture.com/za-en/insights/security/cyberthreat-south-Africa]

[12] *Business Insider South Africa, Hackers on the dark web love South Africa – here's why we suffer 577 attacks per hour*, 23 juin 2020. Consultable à l'adresse : [https://www.businessinsider.co.za/sa-third-highest-number-of-cybercrime-victims-2020-6].

1.1 Méthodologie

Pour réaliser cette évaluation, INTERPOL a cherché à s'appuyer sur les données de ses pays membres en Afrique. Sur les 55 pays membres que compte la région, 22 ont répondu à l'enquête et fait part de leurs perspectives nationales sur les cybermenaces. L'Organisation a également obtenu des données pertinentes de ses partenaires privés, notamment Group-IB, Kaspersky, Palo Alto Networks et Trend Micro. Les informations recueillies ont été combinées aux détections internes et à l'analyse réalisée par la Direction de la Cybercriminalité d'INTERPOL, ainsi qu'à une analyse de sources publiques d'informations, de données et d'évaluations pertinentes pour la région. Cette approche multipartite a permis d'évaluer de manière exhaustive le panorama des cybermenaces dans la région.

Le lancement du projet AFJOC en mars 2021 a été un catalyseur pour la préparation de ce rapport en ce qui concerne la sensibilisation et la coordination avec les pays membres africains d'INTERPOL. En se fondant sur le résultat de l'évaluation, le projet AFJOC va élaborer un cadre opérationnel régional afin de fournir aux pays membres un canevas sur lequel s'appuyer lors du développement de leurs politiques de gouvernance, des rôles et des responsabilités, des procédures, des communications et du renforcement des capacités. Pour ce travail, la collaboration avec les organisations régionales clés comme l'Union africaine et AFRIPOL est fondamentale. Le projet ISPA sous-tend ces relations, collaborations et synergies potentielles.



AFRICA JOINT OPERATIONS AGAINST CYBERCRIME

2. PRINCIPALES CYBERMENACES EN AFRIQUE

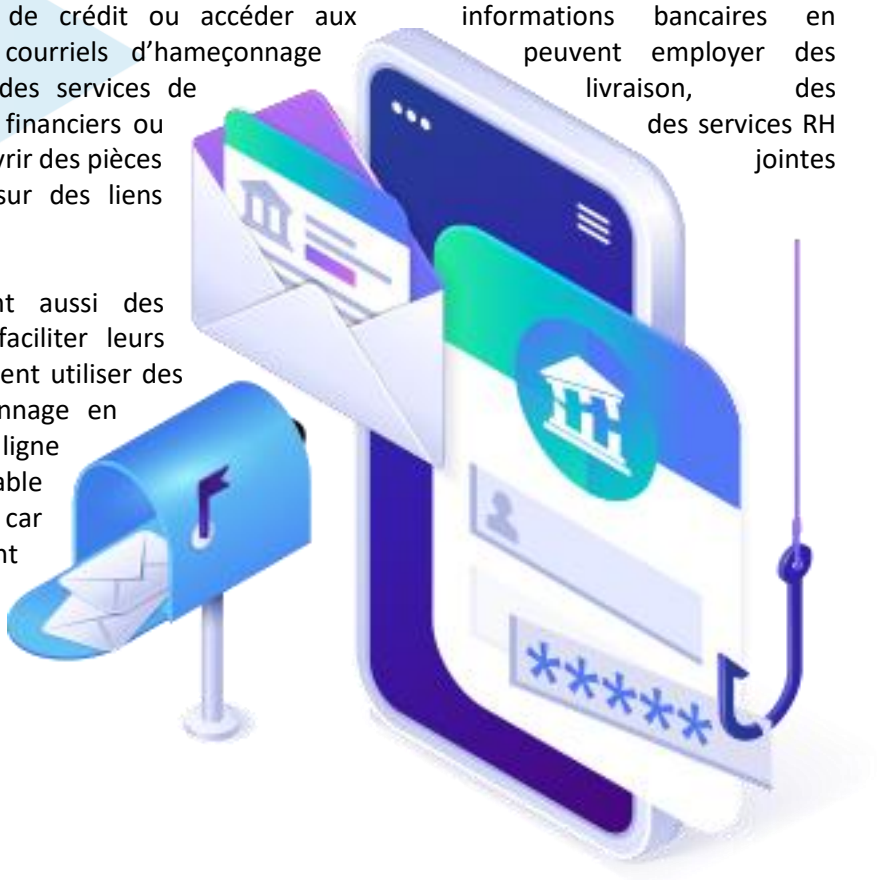
ESCROQUERIES EN LIGNE

2.1 Escroqueries en ligne

Que sont les escroqueries en ligne ?

Les escroqueries en ligne englobent différents types de fraudes réalisées dans le cyberespace. Il s'agit aussi bien de l'hameçonnage que du vol de carte de crédit, de l'usurpation d'identité, de l'escroquerie à l'avance de frais, de la fraude au paiement à distance et des escroqueries aux cybermonnaies. Elles cherchent habituellement à exploiter les peurs, les insécurités ou les vulnérabilités des victimes en employant de multiples tactiques, techniques et procédures (TTP) en ligne. Des groupes criminels organisés complexes utilisent souvent des logiciels malveillants sophistiqués sur mesure pour réaliser des gains financiers illicites au détriment de victimes sans méfiance.

L'escroquerie en ligne la plus répandue est l'hameçonnage. Il peut être réalisé par courriel, SMS, appel téléphonique ou à l'aide d'un kit d'hameçonnage.[13] En ce qui concerne la fraude bancaire et la fraude à la carte de crédit, les acteurs des menaces exploitent les vulnérabilités des systèmes non protégés des banques ou des particuliers, en mettant en œuvre des tactiques d'ingénierie sociale pour obtenir les informations des cartes de crédit ou accéder aux informations bancaires en ligne. Selon Kaspersky, les courriels d'hameçonnage peuvent employer des scénarios mettant en scène des services de livraison, des services postaux, des services financiers ou des services RH et convaincre les victimes d'ouvrir des pièces jointes malveillantes ou de cliquer sur des liens malveillants[14].



Les escrocs en ligne créent aussi des domaines malveillants pour faciliter leurs activités frauduleuses. Ils peuvent utiliser des outils ou des kits d'hameçonnage en masse. Les escroqueries en ligne constituent une stratégie rentable pour les acteurs des menaces, car elles nécessitent un équipement technique minimal et présentent de faibles coûts de démarrage.

[13] Un kit d'hameçonnage est un outil acheté par un acteur de la menace à un autre pour faciliter en masse ses campagnes d'hameçonnage.

[14] Kaspersky, *The year of social distancing or social engineering? Phishing goes targeted and diversifies during COVID-19 outbreak*, août 2020. Consultable à l'adresse : [https://www.kaspersky.com/about/press-releases/2020_the-year-of-social-distancing-or-social-engineering]

Situation en Afrique

Selon les pays membres africains, les escroqueries en ligne constituent la cybermenace la plus prééminente et la plus pressante. En particulier, la fraude bancaire et la fraude à la carte de crédit sont reconnues comme étant une menace grave en Afrique. Elles impliquent le vol de données à caractère personnel et d'informations bancaires qui sont ensuite utilisées par un acteur de la menace pour acheter des biens, siphonner les fonds ou faire de la vente. Conjuguées à la pandémie de COVID-19 et à son impact sur le panorama de la cybercriminalité, les cyberattaques ont enregistré une hausse soutenue en Afrique,[15] notamment une augmentation de 238 % des cyberattaques visant les plateformes bancaires en ligne en 2020.[16]

En parallèle, les acteurs des menaces déploient des chevaux de Troie comme Agent Tesla, Lokibot, Fareit ou d'autres pour voler les informations et commettre des escroqueries en ligne. De nombreux cybermalfaiteurs proposent des boîtes à outils en tant que service et les formations disponibles en ligne ont contribué à pérenniser les opérations et le développement de cette population.

Prenant du champ sur les escroqueries en ligne au sein de la région africaine, les données obtenues de Trend Micro montrent qu'en mai 2021, 27 % de ses détections de menaces sur le Web étaient liés à des escroqueries en ligne, comme indiqué à la Figure 2.

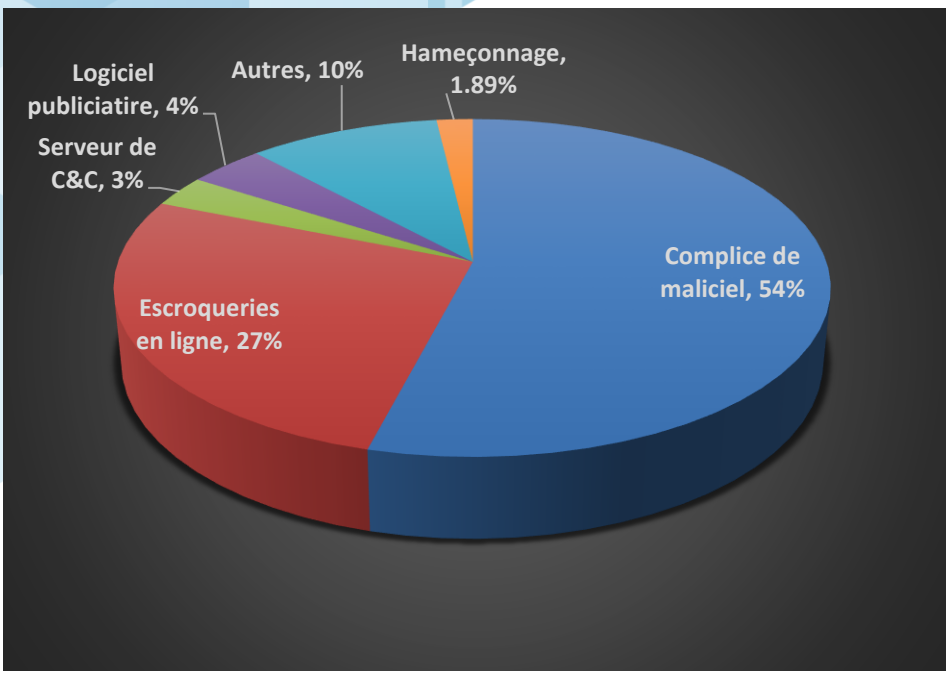


Figure 2 : Détection des principales menaces en ligne en Afrique pour le seul mois de mai 2021 (Source : Trend Micro)

Selon les preuves recueillies par le South African Banking Risk Information Centre (SABRIC), « les pertes brutes dues à la fraude sur les cartes émises en Afrique du Sud ont augmenté de 20,5 % entre 2018 et 2019 » en raison de la fraude au paiement à distance et des attaques de maliciels contre les banques, plaçant le pays juste derrière la Russie.[17] Toutefois, ce chiffre ne tient pas compte des tentatives d'hameçonnage liées à la COVID-19 ni des répercussions financières, émotionnelles et mentales pour les victimes. Les données volées dans le cadre des escroqueries aux cartes de crédit sont vendues aux enchères au plus offrant ou mises en vente sur des forums *underground*. En d'autres termes, les

[15] INTERPOL, Un rapport d'INTERPOL fait état d'un taux de cyberattaques très préoccupant durant le COVID-19, 4 août 2020. Consultable à l'adresse : [https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/Un-rapport-d-INTERPOL-fait-etat-d-un-taux-de-cyberattaques-tres-preoccupant-durant-le-COVID-19]

[16] Institut d'études de sécurité, Africa can't risk a major maritime cyberattack, Reva, D., 28 octobre 2020. Consultable à l'adresse : [https://issafrica.org/iss-today/africa-cant-risk-a-major-maritime-cyber-attack]

[17] *Accenture, Insight Into The Cyber Threat landscape in South Africa*, 2020. Consultable à l'adresse : [https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf]

informations des cartes de crédit des victimes sans méfiance de ce type de fraude en Afrique peuvent être utilisées à mauvais escient n'importe où dans le monde une fois la violation commise.

Selon le rapport 2019 sur l'Afrique de KnowBe4[18], qui a interrogé plus de 800 personnes en Afrique du Sud, au Kenya, au Nigéria, au Ghana, en Égypte, au Maroc, à Maurice et au Botswana, l'hameçonnage est l'une des principales cybermenaces subies par la région africaine. 28,14 % des personnes interrogées ont indiqué avoir déjà cliqué sur un courriel d'hameçonnage, 27,71 % avoir déjà été victime d'une escroquerie et 19 % avoir contribué à faire circuler un courriel non sollicité ou un canular. Kaspersky, l'un des partenaires privés d'INTERPOL, a détecté près de deux millions de tentatives d'hameçonnage en Afrique du Sud, au Kenya, en Égypte, au Nigéria, au Rwanda et en Éthiopie pour la seule année 2020.[19]

Les escroqueries aux cybermonnaies, par lesquelles les acteurs des menaces cherchent à voler les fonds de leurs victimes, constituent un autre sujet de préoccupation croissant pour les pays membres africains. Un rapport de l'IES a mis en exergue deux exemples d'escroquerie aux investissements en cybermonnaies en Afrique du Sud.[20] Le premier est une pyramide de Ponzi mise en place par Mirror Trading International qui aurait permis de voler les bitcoins de milliers d'investisseurs pour un montant équivalant à 588 millions USD en 2020. La deuxième affaire a impliqué les deux fondateurs de la société de trading Africrypt qui ont escroqué leurs investisseurs de 3,6 milliards USD en avril 2021.

L'Afrique du Sud figure de ce fait dans les 10 premiers pays où les acteurs des menaces ont reçu le volume le plus important de cybermonnaies d'adresses illicites. Outre les escroqueries aux investissements, une menace croissante dans l'environnement des cybermonnaies est l'hameçonnage de portefeuille par lequel les acteurs des menaces utilisent des publicités fallacieuses ou trompeuses, de faux domaines, de fausses plateformes de gestion de portefeuille ou de gestion financière décentralisée pour obtenir les clés privées du portefeuille de cybermonnaie de la victime, ce qui leur permet de siphonner ses comptes.

[18] *Knowbe4, African Cybersecurity Research Report*, 2019. Consultable à l'adresse : [https://www.knowbe4.com/hubfs/African%20Cybersecurity%20Research%20Report.pdf]

[19] *Creamer Media's Engineering News, Phishing attacks in Africa diversify, target small companies*, Burger, S., août 2020. Consultable à l'adresse : [https://www.engineeringnews.co.za/article/phishing-attacks-in-Africa-diversify-target-small-companies-2020-08-21]

[20] Institut d'études de sécurité, Afrique : nouvel eldorado d'arnaques aux crypto-arnaques et du blanchiment d'argent, Chelin, R., août 2021. Consultable à l'adresse : [https://issafrica.org/fr/iss-today/afrique-nouvel-eldorado-darnaques-aux-crypto-arnaques-et-du-blanchiment-dargent]

2.2 Extorsion en ligne

EXTORSION EN LIGNE

Qu'est-ce que l'extorsion en ligne ?

L'extorsion en ligne avec chantage et sextorsion a été signalée comme l'une des cybermenaces les plus prééminentes en Afrique. Les acteurs des menaces emploient soit de fausses allégations soit des preuves de données ou de fichiers à caractère personnel volés pour forcer les victimes à payer une rançon afin de les récupérer ou d'éviter leur publication en ligne. Plus spécifiquement, les acteurs des menaces de sextorsion utilisent l'hameçonnage et le chantage sur de nombreuses plateformes pour obtenir de l'argent de leurs victimes en alléguant avoir obtenu des images sexuelles compromettantes ou leur historique de navigation sur des sites à caractère sexuel.

L'analyse d'INTERPOL a identifié le mode opératoire le plus répandu pour l'extorsion en ligne : les acteurs des menaces louent des serveurs privés virtuels (VPS) avec un service SMTP (Simple Mail Transfer Protocol) pour lancer des campagnes en masse de courriels d'extorsion. Les acteurs des menaces y prétendent souvent avoir compromis la sécurité des ordinateurs, des fichiers ou des historiques de navigation de leurs victimes.

Le cyberchantage peut aussi être combiné aux techniques d'ingénierie sociale qui visent à étudier les victimes et à tirer parti des données à caractère personnel qu'elles laissent en ligne sur les billets de médias sociaux ou qui ont été exposées sur les forums du Web de surface ou du dark Web à la suite de violations de données antérieures, dans la mesure où les acteurs des menaces emploient des techniques toujours plus sophistiquées pour créer des messages d'extorsion personnalisés adaptés à chaque victime.

De même, le mode opératoire en cas de sextorsion peut impliquer de fausses allégations d'accès à la webcam ou à l'historique de navigation des victimes, suivies de demandes de paiement en cybermonnaie pour éviter la diffusion de ces informations aux proches ou dans la sphère publique. Même si ces allégations sont souvent produites en masse, des activités de sextorsion ont aussi été détectées via des applications mobiles : les acteurs des menaces trompent les victimes sans méfiance, habituellement des hommes, pour qu'elles s'enregistrent ou envoient des vidéos intimes à des personnes qu'elles pensent être des femmes. Les acteurs des menaces utilisent ensuite ces enregistrements pour faire chanter les victimes si elles veulent éviter leur diffusion.[21]

(Graphic Source: Financial Post)

[21] Trend Micro et INTERPOL, *Cybercrime in West Africa; Poised for an Underground Market*, 2017. Consultable à l'adresse : [https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-Africa.pdf]

Situation en Afrique

Partant de la compréhension du chantage en ligne via l'extorsion, les données communiquées par Trend Micro, un partenaire privé d'INTERPOL, ont identifié certaines adresses IP en Afrique utilisées pour envoyer des courriels non sollicités d'extorsion en ligne. De janvier à mai 2021, les adresses IP uniques dénombrées représentent 10,6 % du nombre total. Les principaux pays d'expédition comprennent l'Afrique du Sud, le Maroc, le Kenya et la Tunisie. Les adresses IP peuvent provenir de réseaux de machines zombies ou de VPS dédiés loués par les cybermalfaiteurs.

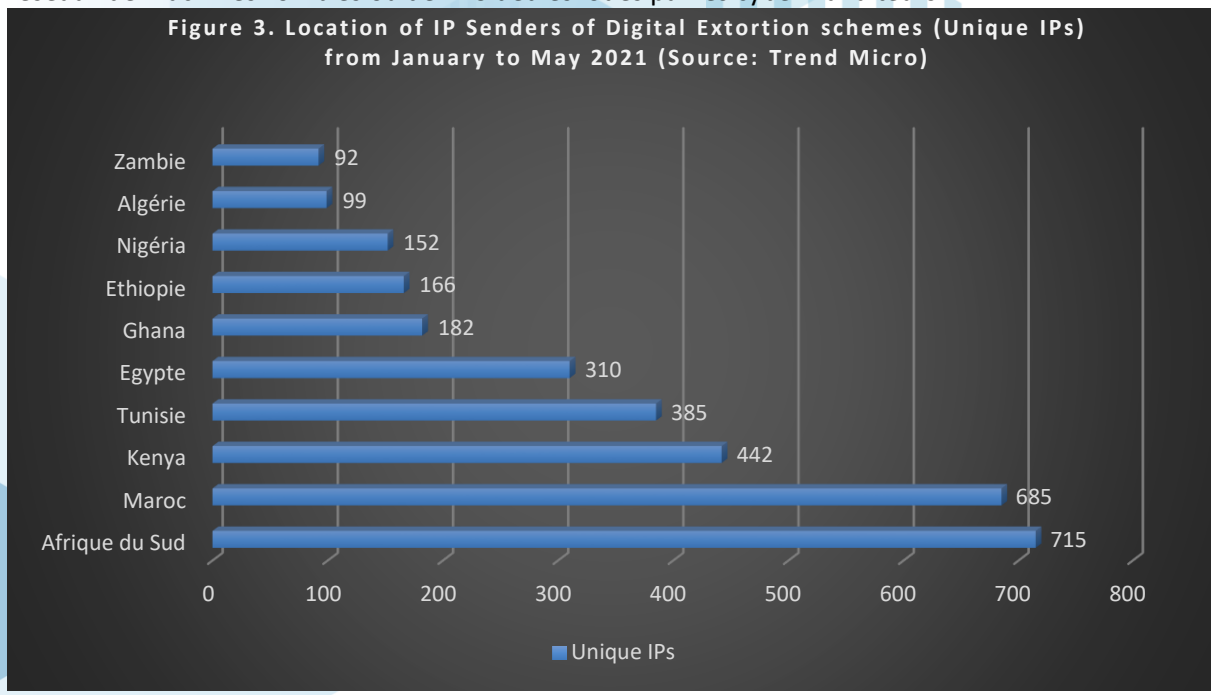


Figure 3. Localisation des IP des expéditeurs de courriels d'extorsion en ligne (IP uniques) entre janvier et mai 2021 (Source : Trend Micro)

Ces données télémétriques de Trend Micro sont conformes au volume de courriels d'extorsion en ligne signalé par les pays membres africains à INTERPOL, ce qui en fait l'une des formes de cybercriminalité les plus signalées dans la région.

2.3 Escroqueries aux faux ordres de virement

ESCROQUERIES AUX FAUX ORDRES DE VIREMENT

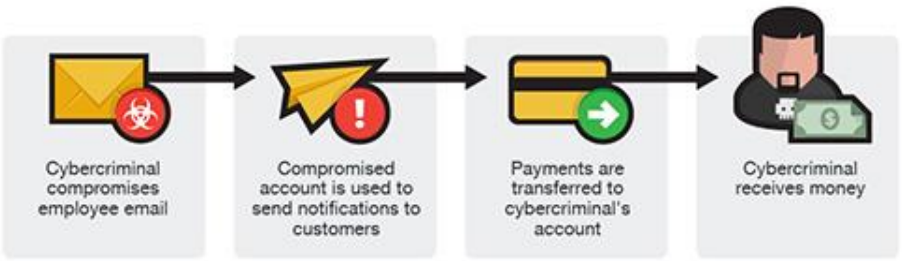
Que sont les escroqueries aux faux ordres de virement ?

Les escroqueries aux faux ordres de virement (FOVI) constituent un type d'escroqueries qui cible les entreprises et les organisations pour obtenir un gain financier ou voler des données. Les cybermalfaiteurs compromettent ou contrefont un compte de messagerie électronique légitime afin d'envoyer des courriels frauduleux demandant le transfert de fonds ou de données sensibles tout en se faisant passer pour le propriétaire légitime.

Les cybermalfaiteurs ciblent habituellement des dirigeants de haut niveau travaillant dans la finance ou s'occupant de paiements par virement bancaire. Ils en compromettent les comptes de messagerie professionnelle par des méthodes comme l'enregistrement de frappe ou des attaques par hameçonnage ou ils en contrefont simplement les courriers électroniques pour donner l'impression qu'ils ont été envoyés du compte de messagerie légitime de la victime. Des courriels frauduleux sont ensuite envoyés depuis ces comptes de messagerie au niveau de confiance établi aux autres salariés ou à des contacts de la victime en leur demandant de transférer des données ou des fonds sur un compte bancaire spécifique. Les trois types d'escroqueries aux FOVI sont présentés dans les infographies ci-dessous réalisées par Trend Micro.

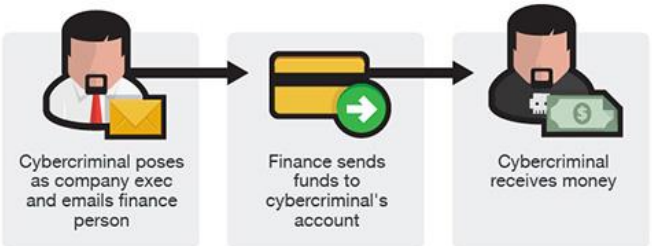
Fraude à la facture fictive

La fraude à la facture fictive implique habituellement une entreprise qui a une relation établie avec un fournisseur. Le fraudeur demande par le biais d'un courriel, d'un appel téléphonique ou d'une télécopie contrefait(e) à ce que le virement dû au titre d'une facture soit réalisé sur un nouveau compte, frauduleux.



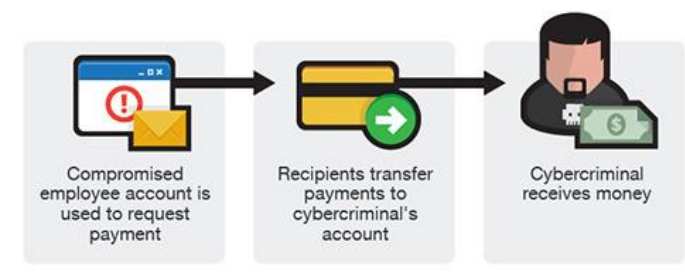
Fraude au président

Dans le cas de la fraude au président, les fraudeurs se présentent comme des dirigeants de haut niveau (DAF, DG, DSI, etc.), des avocats ou d'autres catégories de représentants légaux. Ils prétendent s'occuper d'affaires confidentielles ou contraintes par le temps et demandent un transfert par virement sur un compte qu'ils contrôlent. Dans certains cas, la demande frauduleuse de virement est envoyée directement à l'institution financière avec des instructions pour transférer de manière urgente les fonds à une banque. Cette escroquerie porte différents noms, « fraude au président », « escroquerie au président ».



Compromission de comptes

Dans les cas de compromission de comptes, le compte de messagerie électronique d'un(e) salarié(e) est piraté, puis utilisé pour envoyer des demandes de paiement de factures sur des comptes bancaires contrôlés par le fraudeur. Les messages sont envoyés à plusieurs fournisseurs identifiés dans la liste de contacts de la victime. L'entreprise cliente peut rester dans l'ignorance de cette fraude tant que les fournisseurs ne s'enquièrent pas du statut du paiement de leurs factures.



Pour aider les particuliers et les organisations à se protéger contre les escroqueries aux FOVI, le FBI a aussi publié une liste de signaux d'alerte et de conseils pour reconnaître et contrecarrer les tentatives en la matière (cf. Tableau 1).

Urgence inexpliquée	Accueillir avec scepticisme les changements de dernière minute apportés aux instructions de virement ou aux informations de compte du destinataire.
Changements de dernière minute apportés aux instructions de virement ou aux informations de compte du destinataire	Vérifier les changements apportés aux informations en utilisant les informations de contact enregistrées – ne pas utiliser le numéro indiqué dans le courriel.
Changements de dernière minute apportés aux plateformes de communication établies ou aux adresses de messagerie électronique	Vérifier que l'URL fournie dans le courriel est associée à l'entreprise censée l'avoir envoyée.
Communication uniquement par courriel et refus de communiquer par téléphone, téléphone sur IP ou visioconférence	Faire attention aux hyperliens pouvant contenir le nom réel du domaine, mais mal orthographié.
Demandes inédites de paiement anticipé pour des services	Vérifier l'adresse électronique utilisée pour l'expédition des courriels, en particulier lors de l'utilisation d'un téléphone ou d'un appareil mobile, en s'assurant qu'elle correspond bien à la personne censée l'avoir utilisée.
Demandes de modification des informations de virement direct émanant de salariés	Se méfier des changements de dernière minute apportés aux instructions de virement ou aux informations de compte du destinataire.

Tableau 1 : Signaux d'alerte, bonne pratique et conseils pour éviter les escroqueries aux FOVI (Source : FBI)

Situation en Afrique

Selon Trend Micro, entre 2020 et avril 2021, le pourcentage de tentatives d'escroqueries aux FOVI en Afrique a représenté moins de 1 % des tentatives mondiales. Les pays les plus touchés par ces tentatives appartiennent au monde anglo-saxon comme les États-Unis, l'Australie et le Royaume-Uni. Dans la mesure où les cibles de ces cyberescrocs sont habituellement des entreprises plus importantes susceptibles de leur apporter des gains plus intéressants, la plus faible proportion de tentatives d'escroqueries aux FOVI en Afrique est certainement liée à la concentration relativement moindre de grandes entreprises dans la région.

Toutefois, plusieurs entreprises offshore sont basées en Afrique et la pandémie de COVID-19 a contribué à accroître cette forme de cybercriminalité. Les salariés de ces entreprises dépendent lourdement des transactions par virement bancaire, ouvrant de nouvelles opportunités aux cybermalfaiteurs. En Afrique, les tentatives ont majoritairement été détectées dans des pays comme l'Afrique du Sud, la Tunisie, le Maroc, Maurice, le Nigéria et le Kenya (cf. Figure 4).

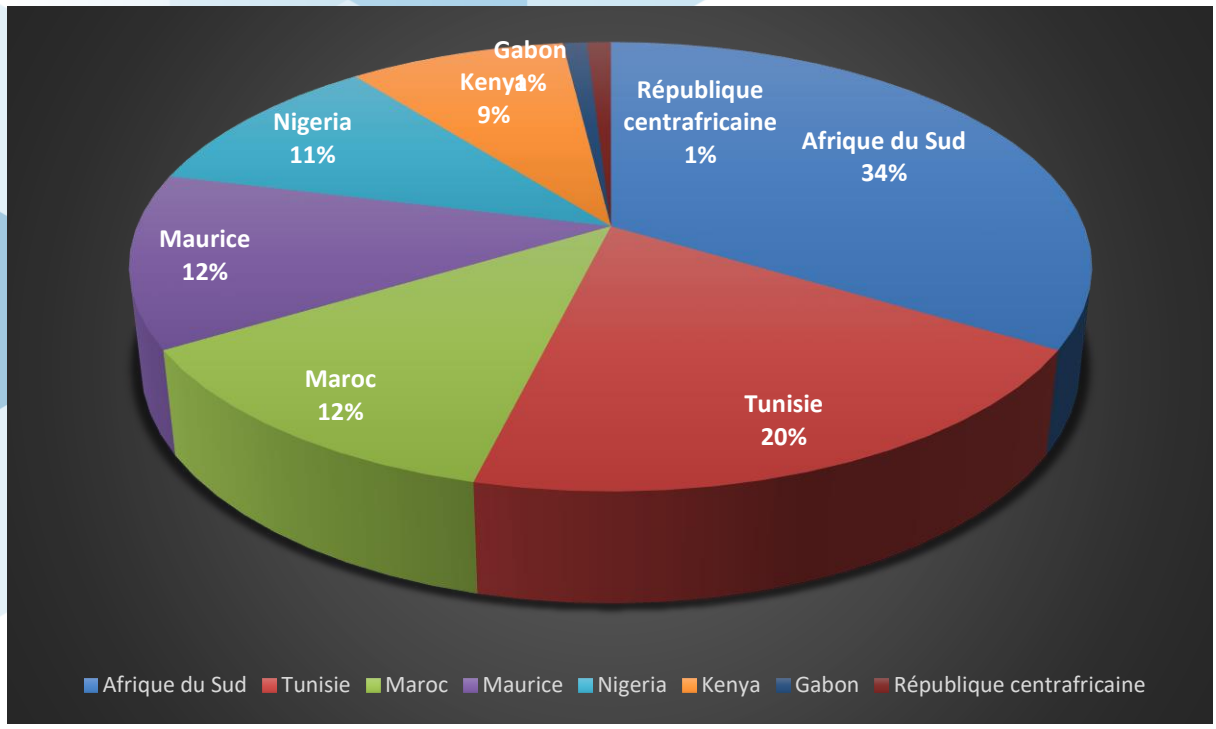


Figure 4. Tentatives d'escroqueries aux FOVI en Afrique (Source : Trend Micro)

Il est probable que ce chiffre augmente, en raison des solides projections économiques positives pour la région africaine. De plus, les statistiques pour 2020 montrent que les pays africains ont survolé le classement des pays affichant la plus forte croissance du PIB dans le monde.[22] Même si la COVID-19 a nettement ralenti la croissance du PIB, les fondamentaux économiques restent en place et confirment la possibilité de voir les acteurs de la menace FOVI cibler davantage la région dans l'espoir de gains supérieurs.

Dans l'intervalle, un rapport publié en 2020 par la division de cyberrenseignement d'Agari (ACID) souligne que la majorité (60 %) des acteurs mondiaux de la menace FOVI sont basés en Afrique, dans 11 pays de la région. Ce rapport signale également que « 83 % des agresseurs africains, et 50 % des acteurs mondiaux de la menace FOVI, provenaient du Nigéria ».[23]

---

[22] *Statista, African countries with the highest Gross Domestic Product* (GDP) in 2020. Consultable à l'adresse : [https://www.statista.com/statistics/1120999/gdp-of-African-countries-by-country/]

[23] *Agari, The Geography of BEC. The Global Reach of the World's Top Cyber Threat*, 2020. Consultable à l'adresse : [https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-geography-of-bec.pdf]

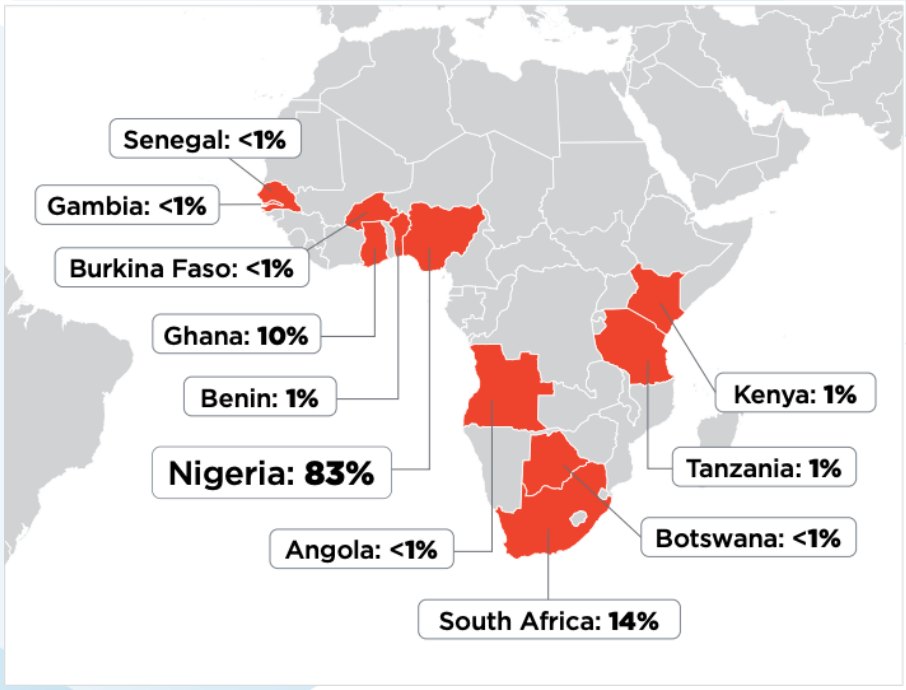


Figure 5 : Répartition des acteurs de la menace FOVI en Afrique (Source : Agari)

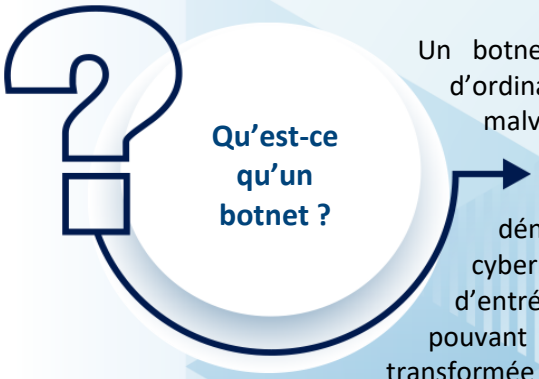
En réponse à la forte concentration d'acteurs de la menace FOVI détectée dans la région nigériane, INTERPOL, appuyée par son partenaire privé Group-IB et par la police nigériane (NPF), a mené avec succès l'opération Falcon qui a permis de désorganiser un groupe prolifique d'escroqueries aux FOVI et de procéder à trois arrestations. Cette action proactive des services chargés de l'application de la loi a aussi conduit à l'arrestation en mars 2021 d'un autre groupe important d'acteurs nigérians de la menace FOVI à la suite d'une enquête diligentée par la Commission nigériane contre les délits économiques et financiers.[24]

En septembre 2019, une opération d'un mois baptisée « Rewired » pilotée par le FBI a permis de désorganiser et de démanteler des campagnes d'escroqueries aux FOVI. Elle s'est traduite par 281 arrestations au Nigéria, en Turquie, au Ghana, en France, en Italie, au Japon, au Kenya, en Malaisie, au Royaume-Uni et aux États-Unis. Elle a aussi permis de saisir près de 3,7 millions USD et de recouvrer près de 118 millions USD de virements frauduleux.[25] Cette opération est un autre exemple démontrant l'importance de la coopération policière internationale pour lutter efficacement contre des campagnes d'escroqueries aux FOVI transitoires.

[24] *Recorded Future, Suspected BEC gang arrested in Nigeria amid internet fraud crackdown efforts*, 2021. Consultable à l'adresse : [https://therecord.media/suspected-bec-gang-arrested-in-nigeria-amid-internet-fraud-crackdown-efforts/]

[25] *FBI, Worldwide Sweep Targets Business Email Compromise*, 10 septembre 2019. Consultable à l'adresse : [https://www.fbi.gov/news/stories/operation-rewired-bec-takedown-091019]

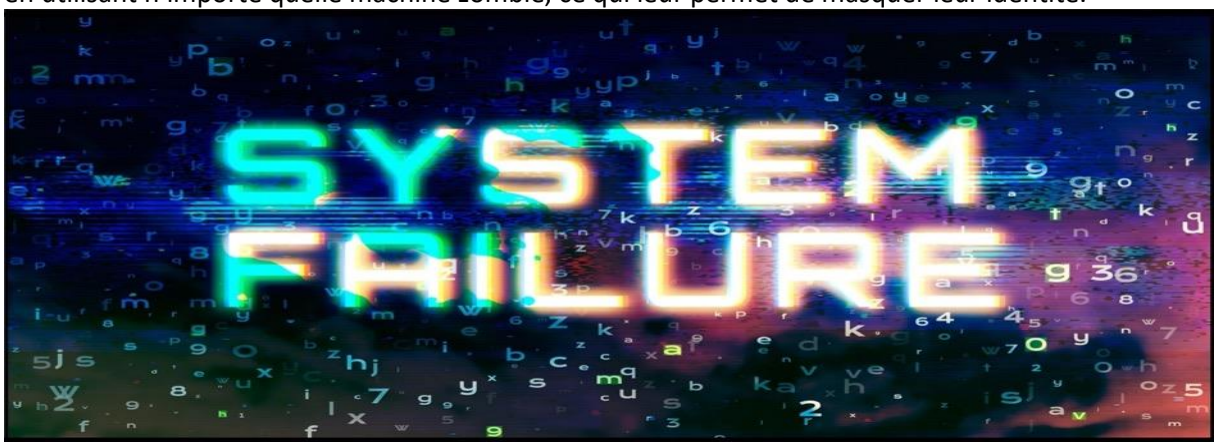
2.4 Botnets



Un botnet, ou réseau de machines zombies, est un réseau d'ordinateurs et de dispositifs piratés et infectés par un robot malveillant, contrôlé à distance par un pirate informatique (cf. Figure 9). Ce réseau peut être utilisé pour envoyer des courriels non sollicités ou pour lancer des attaques par déni de service distribué (DDoS) et il peut être loué à d'autres cybermalfaiteurs. Les botnets peuvent aussi servir de point d'entrée pour les attaques par rançongiciel. Toute machine pouvant se connecter à Internet peut être compromise et transformée en machine zombie : ordinateurs, appareils mobiles, équipements de l'infrastructure Internet comme les routeurs réseau et, de plus en plus, les appareils IdO (Internet des objets) comme les appareils domestiques connectés.

Selon Kaspersky, la construction d'un botnet se fait en trois étapes :[26]

Au moment de l'activation, les pirates informatiques envoient des commandes et contrôlent le botnet à partir d'un serveur central, le serveur de commande et de contrôle (C&C). Les architectures de C&C plus anciennes utilisent un serveur C&C centralisé qui envoie toutes les commandes. Toutefois, comme cela diminue l'anonymat des pirates informatiques, puisqu'il est possible de tracer leurs serveurs C&C, les nouvelles architectures de C&C s'appuient désormais sur une architecture pair à pair décentralisée qui permet aux pirates informatiques d'envoyer et de diffuser les commandes à l'intégralité du botnet en utilisant n'importe quelle machine zombie, ce qui leur permet de masquer leur identité.



[26] Kaspersky, *What is a Botnet*? Consultable à l'adresse : [https://www.kaspersky.com/resource-center/threats/botnet-attacks]

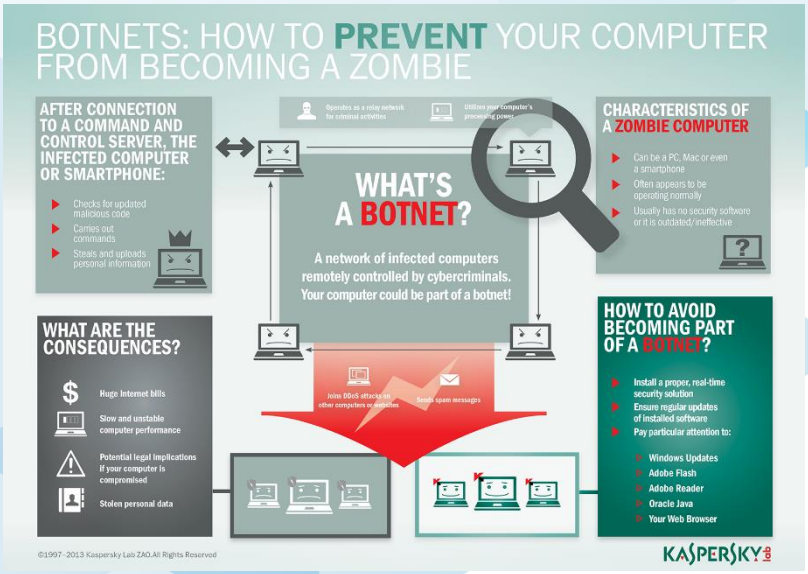


Figure 9 : Présentation générale d'une attaque par un botnet (Source : Kaspersky)

Situation en Afrique

Selon Trend Micro, on détecte en moyenne en Afrique 3 900 victimes de botnets par mois, pour un total d'environ 50 000 détections. Différents acteurs de la menace africains déploient des campagnes de courriels non sollicités en y joignant des chevaux de Troie voleurs comme Emotet, Lokibot, Agent Tesla, Fareit, etc. De manière assez surprenante, la Namibie a présenté le taux de détections le plus élevé pour Emotet, même s'il s'est résorbé après les efforts mondiaux menés plus tôt dans l'année pour désorganiser le botnet Emotet. Les autres principaux logiciels malveillants détectés sont des codes encoquillés (« Web shells »), sorte de portes dérobées, et les vers Dorkbot capables de se propager par le biais des lecteurs amovibles, des courriels et des médias sociaux.

Les cybermalfaiteurs recrutent de nouveaux membres en proposant des formations et en lançant différentes boîtes à outils dédiées à la cybercriminalité. C'est l'une des raisons qui expliquent l'expansion des attaques DDoS, la cybercriminalité en tant que service étant proposée sur le Web de surface et le dark Web. L'expansion des plateformes de communication en ligne a fourni un terreau d'apprentissage aux cybermalfaiteurs, leur permettant de développer et de renforcer leurs compétences, d'apprendre et d'échanger des informations sur les boîtes à outils dédiées à la cybercriminalité et même de partager avec d'autres individus les enseignements tirés, les données volées et les exploits positifs.

De nombreux cas médiatisés de telles attaques DDoS contre des infrastructures essentielles ont eu lieu en Afrique ces cinq dernières années. Ainsi, l'attaque DDoS menée en 2016 par le botnet Mirai au Libéria a paralysé l'infrastructure Internet du pays tout entier, avec des attaques de plus de 500 gigabits par seconde (Gbps), ce qui la place parmi les plus importantes attaques DDoS jamais menées.[27] Plus récemment, en septembre 2019, un grand fournisseur d'accès à Internet (FAI) sud-africain a également été victime d'une attaque DDoS qui l'a paralysé pendant une journée entière.[28]

De même, en octobre 2019 et 2020, les banques sud-africaines ont essuyé une vague soutenue d'attaques DDoS, sans subir de dommages importants. Même si aucun cyberincident important ne s'est récemment produit du fait d'attaques DDoS, celles-ci restent une menace préoccupante contre laquelle les organisations africaines doivent se protéger.

---

27 ZDNET, *'Carpet-bombing' DDoS attack takes down South African ISP for an entire day*. Cimpanu, C. 2019. Consultable à l'adresse : [https://www.zdnet.com/article/carpet-bombing-DDoS-attack-takes-down-south-African-isp-for-an-entire-day/]

28 *CPO Magazine, Sustained DDoS Attack on South African Banks Accompanied by Ransom Notes*. Ikeda, S. 2019. Consultable à l'adresse : [https://www.cpomagazine.com/cyber-security/sustained-DDoS-attack-on-south-African-banks-accompanied-by-ransom-notes/]

2.5 RANÇONGICIELS

RANÇONGICIELS

Qu'est-ce qu'un rançongiciel ?

Un rançongiciel est un logiciel malveillant qui crypte les données de la victime ou verrouille ses systèmes, désorganisant les opérations des organisations victimes en rendant leurs données et leurs systèmes inaccessibles. Les opérateurs des rançongiciels demandent ensuite une rançon, habituellement en cybermonnaie pour des raisons d'anonymat, en échange du décryptage des données. Il est à noter que le déploiement du code des rançongiciels sur le réseau d'une organisation fait suite à une violation de ce réseau par un acteur légitime (personne interne de confiance) ou illégitime, à l'exploration du réseau par les cybermalfaiteurs et au vol des informations et des données de l'organisation. Le déploiement d'un rançongiciel est généralement la phase finale d'un piratage ou d'une pénétration réussi(e) du réseau de l'organisation.

Avec la complexification des TTP, la facilitation des attaques par rançongiciel par les groupes criminels organisés s'est élargie pour inclure les doubles et triples extorsions : l'attaque par rançongiciel initiale est démultipliée par le vol de données sensibles de l'entreprise, des demandes de rançon aux victimes en les menaçant de les humilier publiquement par la diffusion des informations volées, et la réexploitation des vulnérabilités exposées par le passé, ce qui soumet les organisations à un cycle sans fin d'attaques par rançongiciel.

Capables d'interrompre instantanément l'activité des administrations, des entreprises et des chaînes d'approvisionnement, les attaques par rançongiciel se traduisent aussi par un impact sur la réputation des victimes, sans oublier les répercussions économiques, ainsi que le montrent les études réalisées par Palo Alto Networks, un partenaire privé d'INTERPOL, qui révèle que les rançons moyennes versées atteignent désormais plus de 300 000 USD.[29]

Cet impact est aggravé du fait de l'adoption croissante de TTP par les groupes criminels organisés, entraînant la suppression de fichiers et de sauvegardes cruciaux qui s'ajoute au temps d'immobilisation moyen estimé de 21 jours par attaque par rançongiciel[30]. Dans la mesure où les recherches indiquent qu'une attaque par rançongiciel se produit toutes les 11 secondes, et au regard des cybervulnérabilités déjà présentées fragilisant la région africaine, il n'a jamais été aussi urgent de comprendre, de manière exhaustive, la situation des attaques par rançongiciel en Afrique et de mettre en œuvre les principes de prévention et de protection.

[29] *Palo Alto Networks, Extortion Payments Hit New Records as Ransomware Crisis Intensifies*, Baylor, Brown et Martineau, août 2021. Consultable à l'adresse : [https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/]

[30] *Forbes, Ransomware is everywhere*, Durbin, S., 2021. Consultable à l'adresse : [https://www.forbes.com/sites/forbesbusinesscouncil/2021/06/01/ransomware-is-everywhereheres-what-you-need-to-consider/?sh=1ded127c1f0f]

Situation en Afrique

Selon les études de Kaspersky, plus de 1,5 million de détections de rançongiciel ont été recensées en 2020. Au cours du premier trimestre 2021, l'Égypte, l'Afrique du Sud et la Tunisie ont été les pays les plus touchés de toute la région, et l'Égypte a subi à elle seule près de 35 % des détections de rançongiciels en Afrique (cf. Tableau 2).

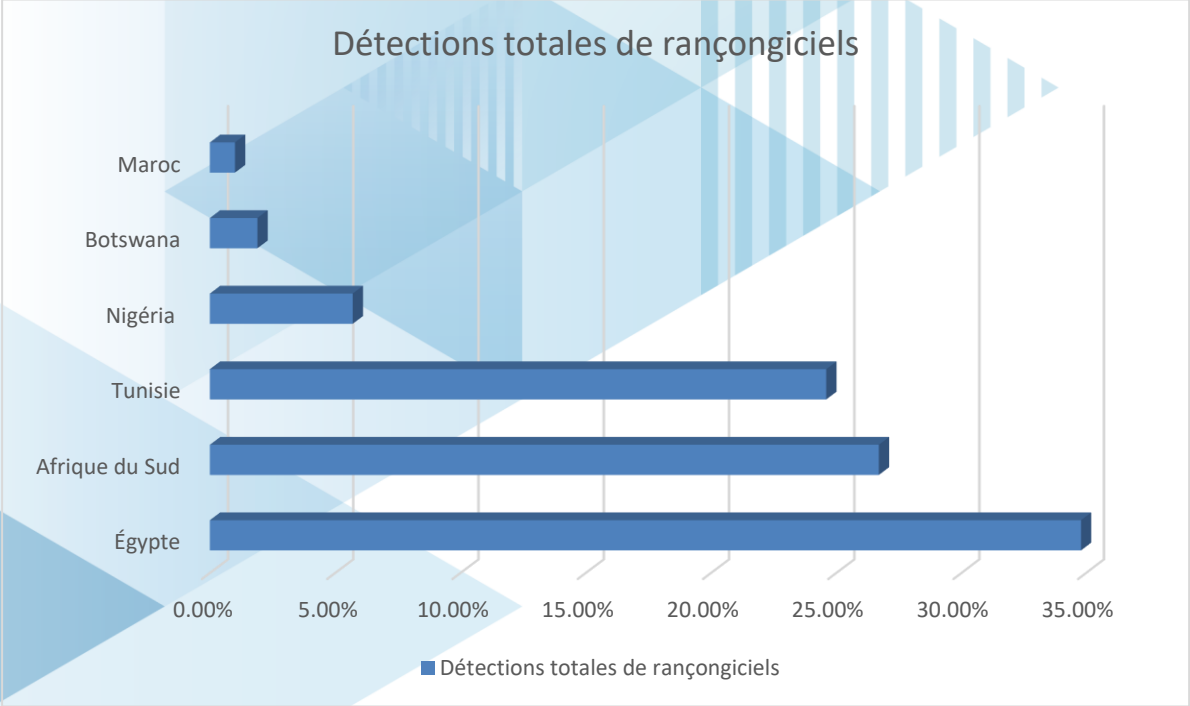


Tableau 2 : Détections de rançongiciels en Afrique en mars 2021 (Source : Trend Micro)

Même si le ratio de détections totales de rançongiciels en Afrique place la région en bas de tableau par rapport aux autres régions du monde, dans les 10 derniers pour cent, selon les analyses de Check Point Software Technologies, les organisations africaines ont subi la « hausse d'attaques la plus importante, à 34 % » entre janvier et avril 2021.[31] Comme l'a indiqué le Centre d'études stratégiques de l'Afrique en janvier 2021, « Au fur et à mesure de la pénétration grandissante d'Internet et de l'interconnexion accrue des systèmes, les infrastructures critiques d'Afrique sont de plus en plus à la merci de cyberattaques qui pourraient s'avérer coûteuses et pernicieuses ».[32]

En Afrique, Wannacry reste un rançongiciel privilégié et les cybermalfaiteurs élargissent également leurs opérations pour passer à la double extorsion. Un exemple est donné par le célèbre rançongiciel Nefilim qui s'attaque au secteur bancaire et aux administrations publiques.

[31] *Checkpoint, The New Ransomware Threat: Triple Extortion*, 2020. Consultable à l'adresse : [https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/]

[32] Centre d'études stratégiques de l'Afrique, L'Afrique à l'épreuve des nouvelles formes de cybercriminalité. Allen, N. février 2021. Consultable à l'adresse : [https://africacenter.org/fr/spotlight/lafrique-a-lepreuve-des-nouvelles-formes-de-cybercriminalite/]

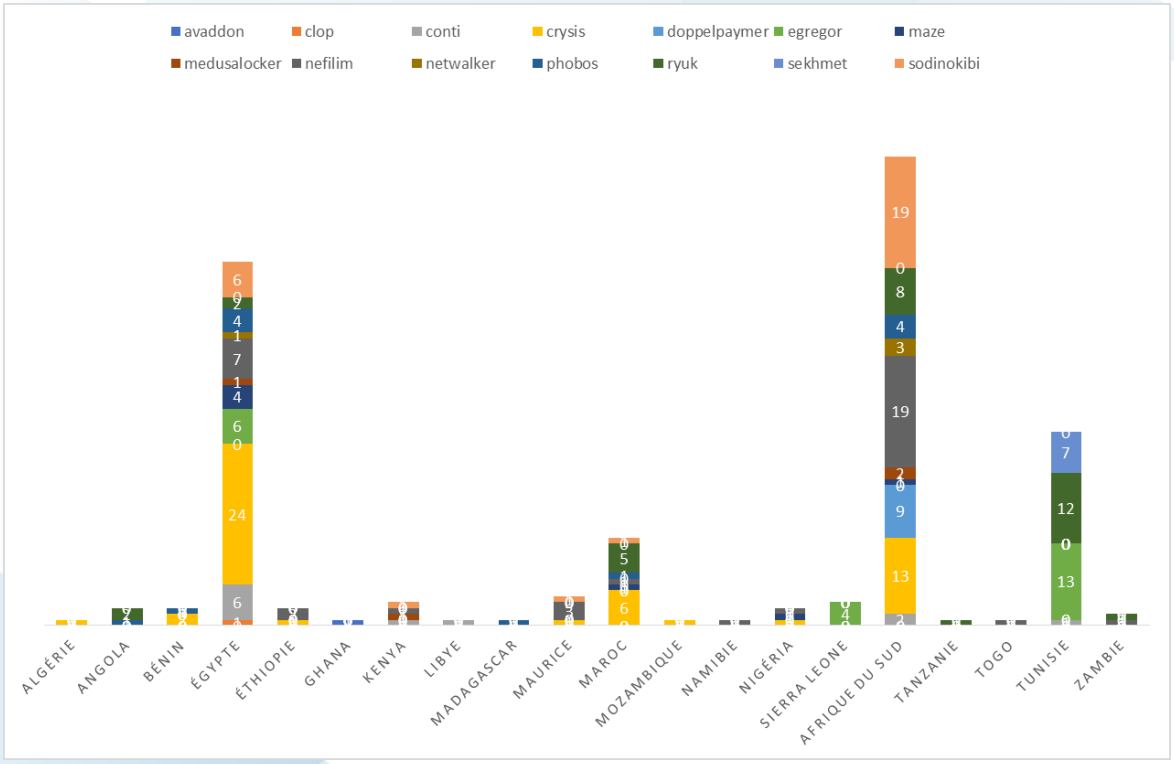


Figure 6. Rançongiciels ciblés en Afrique, détections uniques et familles sélectionnées (Source : Trend Micro)

Selon la Figure 6 ci-dessus, au cours du premier trimestre 2021, l'Afrique du Sud a été le pays le plus fortement touché par les rançongiciels ciblés issus d'un large éventail de familles comme les rançongiciels Crysis, Nefilim, Ryuk, Clop, et Conti. L'Égypte a été le deuxième pays le plus touché avec un profil similaire dans les détections de rançongiciels ciblés. La Tunisie se place en troisième position et a été principalement ciblée par les rançongiciels Egregor (avant son démantèlement en février 2021) Ryuk et Sekhmet.

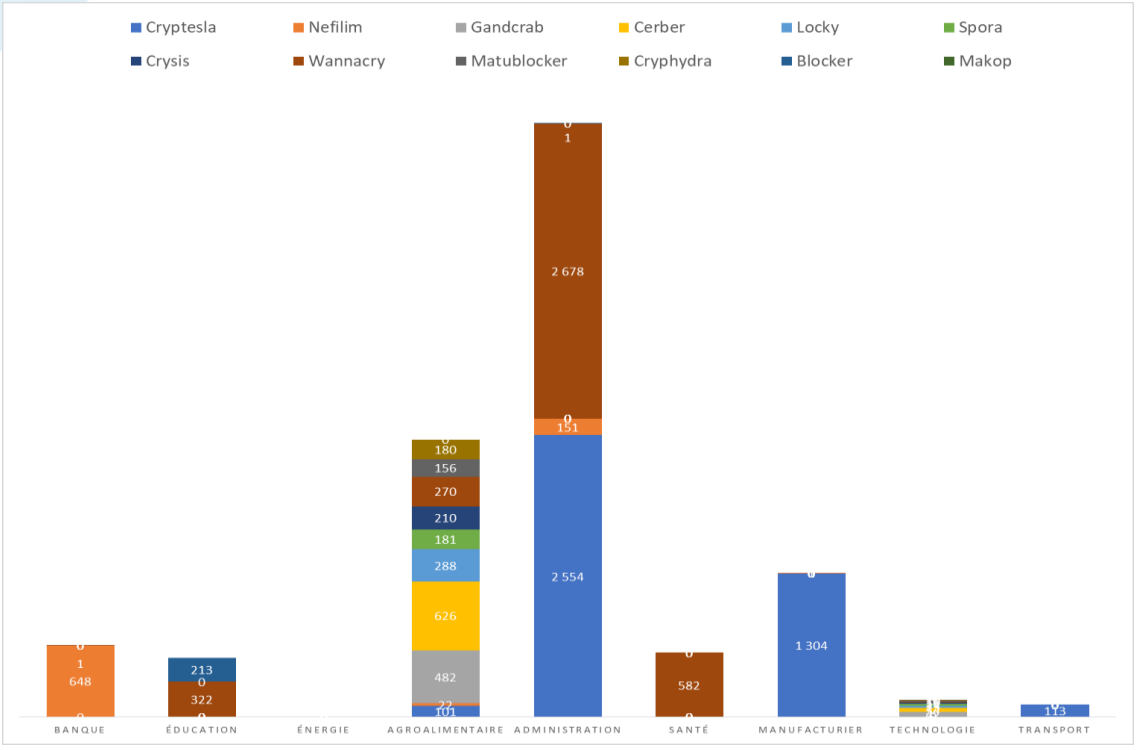


Figure 7. Secteurs touchés par les rançongiciels en Afrique entre le 1er janvier et avril 2021 (Source : Trend Micro)

Selon Trend Micro, les secteurs les plus touchés en Afrique sont les administrations publiques et le secteur agroalimentaire (cf. Figure 7). Selon les observations menées, la prévalence du rançongiciel Wannacry dans les administrations publiques s'explique par le nombre important de machines qui présentent toujours la vulnérabilité du protocole SMB (Server Message Block) connue pour être ciblée par ce rançongiciel.

Il existe également de nombreuses familles de rançongiciels plus anciennes comme Cerber, Gandcrab, Locky, Cryptesla qui ciblent les administrations publiques, le secteur agroalimentaire et l'industrie manufacturière. Une exception notable est le célèbre rançongiciel Nefilim plus récent, découvert en mars 2020,[33] qui cible le secteur bancaire africain.

La motivation des opérateurs de rançongiciels étant le profit, le problème subsistera à l'échelle mondiale tant que les organisations victimes seront disposées à payer les rançons ou forcées de le faire. Comme l'a indiqué le Brookings Institution en mars 2021, en Afrique, les cybermenaces sont exacerbées par les vulnérabilités des stratégies publiques de cybersécurité et par l'impact économique de la pandémie de COVID-19.[34]

"Les cybercriminels développent et intensifient leurs attaques à un rythme alarmant, exploitant la peur et l'incertitude causées par la situation sociale et économique instable créée par COVID-19. "

Jürgen Stock, INTERPOL Secretary General

[33] *Trend Micro, An Analysis of the Nefilim Ransomware*. Février 2021, Agcaoili, Gelera. Consultable à l'adresse : [https://www.trendmicro.com/en_us/research/21/b/nefilim-ransomware.html]

[34] *Brookings, How African states can improve their cybersecurity*, Signé et Signé, 16 mars 2021. Consultable à l'adresse : [https://www.brookings.edu/techstream/how-African-states-can-improve-their-cybersecurity/]

EXEMPLES D'ATTAQUES CONTRE DES INFRASTRUCTURES ESSENTIELLES EN AFRIQUE

- En Afrique du Sud, l'organisation Life Healthcare, le deuxième plus important opérateur hospitalier privé, en charge de la gestion des services numériques d'hôpitaux du pays, a été touchée par une cyberattaque en juin 2020.[32] Cette attaque, menée en pleine pandémie de COVID-19, a affecté ses systèmes de gestion des admissions, ses systèmes de traitement administratif et ses serveurs de messagerie électronique et l'a contrainte à mettre certains de ses systèmes hors ligne. Cette attaque lui aurait coûté plus d'un mois de temps d'immobilisation en pleine pandémie.
- Les attaques jumelles qui se sont produites à Johannesburg en octobre 2020 ont commencé par la mise à l'arrêt de services sociaux essentiels de la ville, notamment les services de paiement de factures, de conseil social et les services d'urgence, à la suite d'une violation de données et se sont poursuivies par le déploiement d'un rançongiciel. L'analyse de l'attaque a identifié non seulement l'exploitation d'une vulnérabilité, mais aussi, après l'utilisation de techniques de mouvement latéral, le déploiement délibéré du rançongiciel pour coïncider avec le cycle de paiement « de fin de mois » dans un effort pour forcer encore plus les autorités sud-africaines à payer la rançon en cybermonnaie.[33]
- Au Kenya, une attaque a ciblé les marchés et les cybersystèmes interconnectés et INTERPOL a averti que les attaques contre les chaînes d'approvisionnement pourrait bien définir le panorama des cybermenaces au cours de la prochaine décennie. Des attaques médiatisées menées contre les chaînes d'approvisionnement, avec la compromission du service informatique de Kaseya par le groupe de rançongiciel REVIL[34], affectent en particulier les clients au Kenya.
- Une attaque DDoS a été menée contre les banques sud-africaines, programmée là encore pour toucher et désactiver les services lors du cycle de paiement « de fin de mois ». Cette attaque a été lancée contre plusieurs grandes banques en Afrique du Sud et s'est une nouvelle fois assortie d'une demande de rançon en cybermonnaie. Même si le préjudice lié à cette attaque a été minime, entraînant simplement une perturbation des services, cette attaque et la double attaque par rançongiciel à Johannesburg soulignent l'ampleur, l'impact et la gravité de la menace pour les infrastructures essentielles en Afrique.
- L'organisation publique sud-africaine Transnet a essuyé une cyberattaque sans précédent en juillet 2021, qui a fortement perturbé ses services.[35] L'Institut d'études de sécurité (IES) a souligné le fait que « l'intégrité de l'infrastructure maritime essentielle du pays a, pour la première fois, fait l'objet d'une désorganisation grave ». Cette attaque contre les installations portuaire a permis de retarder ou de fermer une route commerciale essentielle et de désorganiser des services commerciaux vitaux en pleine pandémie mondiale. L'attaque aurait suspendu le fonctionnement de l'installation de gestion automatisée en ligne des conteneurs tant à Cape Town qu'à Durban, ce dernier étant le port le plus actif d'Afrique subsaharienne et une plateforme maritime pour l'acheminement de marchandises essentielles destinées à d'autres pays africains, notamment la Zambie et la République démocratique du Congo.

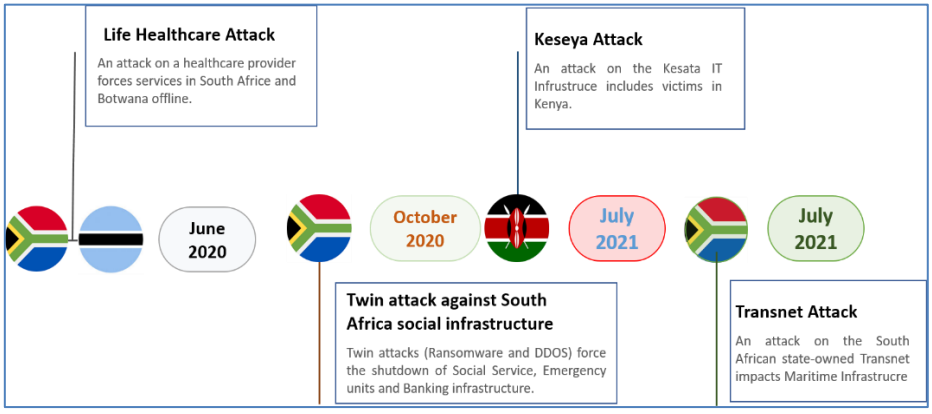


Figure 8. Principaux incidents critiques publiquement documentés en Afrique pour la période 2020-2021

3. SUCCES OPERATIONNELS

Au titre de son mandat pour réduire l'impact mondial de la cybercriminalité et protéger les communautés pour un monde plus sûr, la Direction de la Cybercriminalité d'INTERPOL fournit des capacités policières à tous les pays membres de l'Organisation par le biais du Programme mondial de lutte contre la cybercriminalité qui se compose de trois volets : i) la réponse aux cybermenaces, ii) le renforcement de la cyberstratégie et des cybercapacités et iii) les cyberopérations.

Le premier volet, « Réponse aux cybermenaces », identifie, calibre et coordonne de manière ciblée et spécifique la réponse mondiale apportée aux cybermenaces, en s'appuyant sur l'expertise des partenaires privés et les données sur la cybercriminalité. Il cherche à développer le renseignement sur les menaces identifiées afin de concevoir des stratégies de perturbation et de prévention qui atténuent les cybermenaces à haut risque et à impact élevé. Il vise également à fournir des conseils et des orientations de qualité concernant l'état actuel de la menace, ainsi qu'un soutien opérationnel grâce à la communication de renseignements exploitables.

Le volet « Renforcement de la cyberstratégie et des cybercapacités » appuie les pays membres en les dotant de compétences, de connaissances et de capacités techniques en matière de lutte contre la cybercriminalité adaptées à leurs besoins, dans le respect des normes de l'Organisation. En collaboration avec ses parties prenantes, l'équipe planifie, élabore et met en œuvre des projets et des programmes de renforcement des capacités et des cybercapacités, ainsi que des outils et des plateformes, afin de permettre aux pays membres de mieux lutter contre la cybercriminalité au niveau mondial.

Le volet « Cyberopérations » pilote et coordonne les activités opérationnelles transnationales avec les pays membres pour agir contre les cybermenaces à l'origine de préjudices importants aux niveaux national, régional et mondial. En étroite coopération avec les pays membres, les secteurs public/privé et les communautés des cellules de réponse aux attaques informatiques (CERT), il procède à des activités opérationnelles visant les actes de cybercriminalité à fort impact par le biais de l'approche du « Desk régional pour les opérations conjointes de lutte contre la cybercriminalité ».

En mai 2021, INTERPOL a établi un nouveau Desk régional pour les opérations conjointes de lutte contre la cybercriminalité afin d'accroître les capacités de lutte contre la cybercriminalité de 49 pays africains sous l'égide du projet AFJOC. Ce Desk africain pour les opérations conjointes de lutte contre la cybercriminalité aidera à concevoir une stratégie régionale afin de piloter des actions de lutte contre les cybermalfaiteurs coordonnées et fondées sur le renseignement et d'appuyer les opérations conjointes. Les deux opérations présentées ci-dessous ont permis de fournir un appui opérationnel opportun et efficace aux pays membres africains.

3.2 Opération Lyrebird

En 2021, un présumé cybermalfaiteur très actif a été appréhendé au Maroc à la suite d'une enquête de deux ans menée conjointement par INTERPOL, la police marocaine et Group-IB. Agissant sous le pseudonyme de « Dr Hex », le suspect aurait, des années durant, ciblé des milliers de victimes sans méfiance en se livrant à l'hameçonnage, à la fraude et au piratage de cartes bancaires à l'échelle mondiale.

Il est aussi accusé de s'être livré au « défacement » de nombreux sites Web en en modifiant la présentation et le contenu, et d'avoir ciblé des entreprises de télécommunications francophones, plusieurs banques et des multinationales en utilisant des logiciels malveillants. Par ailleurs, le suspect aurait contribué à développer des kits de piratage de cartes bancaires et d'hameçonnage, qui étaient ensuite vendus à d'autres individus via des forums en ligne, afin de leur permettre de mener des campagnes similaires de maliciels.

Les logiciels malveillants étaient ensuite utilisés pour usurper l'identité de banques en ligne, ce qui a permis au suspect et à d'autres de voler des informations sensibles et d'escroquer des personnes sans méfiance à des fins de profit. Le préjudice causé aux particuliers et aux entreprises était ensuite publié sur Internet, afin de faire la publicité de ces services malfaisants.

Dans le cadre de l'opération Lyrebird, la Direction de la Cybercriminalité d'INTERPOL a travaillé en étroite coopération avec Group-IB et la police marocaine par l'intermédiaire du Bureau central national du Maroc à Rabat, pour enfin localiser et appréhender l'individu, qui fait toujours l'objet d'une enquête.

3.3 Opération Falcon

Dans le cadre de l'opération Falcon, trois suspects ont été arrêtés à Lagos en novembre 2020 à la suite d'une enquête menée conjointement par INTERPOL, Group-IB et la police nigériane. Ces ressortissants nigérians sont soupçonnés d'être membres d'un vaste groupe criminel organisé responsable de la diffusion de logiciels malveillants, de la mise en œuvre de campagnes d'hameçonnage et de la commission de nombreuses escroqueries aux faux ordres de virement.

Les suspects auraient mis au point des liens d'hameçonnage, des noms de domaines utilisés pour l'hameçonnage et des campagnes d'envoi massif de messages électroniques dans lesquels ils usurpaient l'identité de représentants d'organisations. Ces campagnes ont permis la diffusion de 26 logiciels malveillants, logiciels espions et outils de prise de contrôle à distance, comme Agent Tesla, Loki, Azorult, Spartan et les chevaux de Troie d'accès à distance Nanocore et Remcos. Ces programmes étaient utilisés pour infiltrer et surveiller les systèmes des organisations et des particuliers victimes avant de lancer les escroqueries et de siphonner les fonds.

Selon Group-IB, la bande organisée prolifique pourrait avoir compromis les systèmes d'entreprises publiques et de sociétés privées dans plus de 150 pays depuis 2017. Au cours de l'enquête qui a duré une année, la Direction de la Cybercriminalité et l'unité Criminalité financière d'INTERPOL ont collaboré étroitement avec Group-IB pour identifier et localiser les menaces et, le moment venu, appuyer la police nigériane, par l'intermédiaire du Bureau central national INTERPOL du Nigéria à Abuja, afin de prendre rapidement des mesures.

INTERPOL | THE NIGERIA POLICE | GROUP-IB

4. STRATEGIE REGIONALE INTERPOL DE LUTTE CONTRE LA CYBERCRIMINALITE POUR L'AFRIQUE

INTERPOL propose une stratégie régionale de lutte contre la cybercriminalité pour l'Afrique qui sous-tend le cadre opérationnel du Desk africain pour les opérations conjointes de lutte contre la cybercriminalité. Venant en appui des activités de ce Desk, la stratégie englobe quatre objectifs stratégiques présentés ci-dessous.

Objectif stratégique N° 1 :
Renforcer le renseignement sur la cybercriminalité afin d'y apporter des réponses efficaces

Objectif stratégique N° 2 :
Renforcer la coopération pour les opérations conjointes de lutte contre la cybercriminalité

Objectif stratégique N° 3 :
Développer les capacités et les moyens de la région pour lutter efficacement contre la cybercriminalité

Objectif stratégique N° 4 :
Promouvoir une bonne cyberhygiène et la résilience afin de rendre le cyberespace plus sûr

Le Desk africain pour les opérations conjointes de lutte contre la cybercriminalité mis en place au titre du projet AFJOC traitera les affaires de cybercriminalité en appui de la région africaine par le biais des piliers stratégiques suivants :

- **[Objectif 1] Renforcer le renseignement sur la cybercriminalité afin d'y apporter des réponses efficaces**

  Au titre du cadre de partenariat du projet Gateway, INTERPOL va collaborer avec des entités privées afin de demander et de recevoir des informations à jour sur les menaces, les tendances et les risques en matière de cybercriminalité au sein de la région africaine. En traitant et en analysant ces informations au moyen d'outils développés en interne ou par des entités extérieures, l'Organisation sera en mesure de mieux comprendre le panorama des menaces liées à la cybercriminalité, et ainsi de produire des cyberrenseignements et des réponses aux menaces opportuns et précis au bénéfice des pays membres africains.

- **[Objectif 2] Renforcer la coopération pour les opérations conjointes de lutte contre la cybercriminalité**

  En étroite coopération avec les pays membres, les partenaires privés et les communautés des cellules de réponse aux attaques informatiques (CERT), INTERPOL va, par le biais du Desk africain pour les opérations conjointes de lutte contre la cybercriminalité, renforcer la coopération et augmenter le nombre d'opérations conjointes ciblant des actes de cybercriminalité à fort impact.

- **[Objectif 3] Développer les capacités et les moyens régionaux de lutte contre la cybercriminalité**

  En collaboration avec ses parties prenantes, INTERPOL va planifier, élaborer et mettre en œuvre des projets et des programmes de renforcement des capacités et des cybercapacités afin de permettre aux pays membres de mieux lutter contre la cybercriminalité en Afrique. Dans le cadre de cet effort, l'Organisation va maximiser l'utilisation des outils et des plateformes comme l'outil d'Échange de connaissances sur la cybercriminalité, la plateforme collaborative sur la cybercriminalité - Opérations et la plateforme du Centre de fusionnement sur la cybercriminalité.

- **[Objectif 4] Promouvoir une bonne cyberhygiène afin de rendre le cyberespace plus sûr**

  INTERPOL va procéder à une campagne de sensibilisation mondiale pour mieux sensibiliser le public aux grandes cybermenaces et promouvoir une bonne cyberhygiène pour les particuliers et les entreprises installés en Afrique. Cette campagne appuiera également les efforts régionaux de prévention et d'atténuation mis en œuvre par les services chargés de l'application de la loi pour cibler les principales cybermenaces, en vue d'en tirer de meilleurs résultats.

Le Desk africain pour les opérations conjointes de lutte contre la cybercriminalité va servir de canal entre les communautés des services chargés de l'application de la loi de la région et le secteur privé pour réaliser ces objectifs et développer davantage le cadre opérationnel en vue d'améliorer les actions coordonnées de lutte contre la cybercriminalité menées en Afrique.

CONCLUSION

Dans ce rapport 2021 d'évaluation des cybermenaces en Afrique, nous nous sommes attachés à présenter le contexte des cybermenaces en Afrique et à en analyser le panorama en nous concentrant sur les cinq principales menaces. Ces menaces affectent également les autres régions, confirmant la nature sans frontières de la cybercriminalité. L'enjeu spécifique à l'Afrique semble être l'absence critique de protocoles de cybersécurité, de cyberrésilience ainsi que de mesures de prévention et d'atténuation pour les particuliers et les entreprises. En tant que région embrassant la transformation numérique, l'Afrique doit investir massivement pour améliorer la sécurité et la sûreté du cyberespace.

Nous soulignons aussi dans ce rapport l'appui contre les cybermenaces qu'INTERPOL apporte à ses pays membres en coordonnant les opérations de lutte contre la cybercriminalité qui ont déjà conduit à l'identification et à l'arrestation d'acteurs des menaces en collaboration avec ses partenaires privés. Les conclusions de cette évaluation peuvent encourager les pays membres à prioriser et à allouer des ressources pour lutter contre la cybercriminalité afin de renforcer ces activités opérationnelles et d'obtenir de meilleurs résultats.

En raison de la nature très changeante et transnationale de la cybercriminalité, seule une réponse coordonnée et rapide permet de la combattre efficacement. Le recueil et l'échange de renseignements sont vitaux pour une réponse efficace des services chargés de l'application de la loi. INTERPOL dispose de la capacité de renseignement nécessaire par le biais de l'équipe Réponse aux cybermenaces et par l'établissement du Desk africain pour les opérations conjointes de lutte contre la cybercriminalité.

Dans ce contexte, les pays membres devraient s'appuyer sur la coopération au niveau policier et en maximiser l'utilisation par l'intermédiaire des canaux, des plateformes et des capacités de l'Organisation pour une réponse opportune et efficace. Les efforts collectifs dans l'échange de renseignements et la formulation d'un cadre opérationnel conjoint renforceront les capacités et les moyens régionaux de lutte contre la cybercriminalité. Partant de ce constat, nous présentons aussi dans ce rapport la stratégie régionale INTERPOL de lutte contre la cybercriminalité pour l'Afrique qui servira de fondation au cadre opérationnel conjoint à développer pour la région.

Les services chargés de l'application de la loi doivent être un partenaire de confiance, en raison de l'importance primordiale du partage des données, notamment entre les polices nationales et avec les secteurs public et privé. Alors que la communauté internationale est soumise à une pression exceptionnelle, renforcer notre sécurité commune exige de notre part une plus grande collaboration. Avec ses pays membres et ses partenaires, INTERPOL continuera à limiter l'impact de la cybercriminalité et à protéger les communautés pour un monde plus sûr.

Contributeurs INTERPOL

Wookyung Jung, Analyste en politique, Direction de la Cybercriminalité

Richard Lim, Chef de projet, Desk africain pour les opérations conjointes de lutte contre la cybercriminalité

Emmanuel Kabera, Officier de renseignement sur la cybercriminalité, Desk africain pour les opérations conjointes de lutte contre la cybercriminalité

Mohammed Isah, Officier en cyberopérations, Cyb Desk africain pour les opérations conjointes de lutte contre la cybercriminalité

Shane Cross, Chef par intérim de l'unité de renseignement sur la cybercriminalité, Réponse aux cybermenaces

Joyce Sin, Officier de renseignement sur la cybercriminalité, Réponse aux cybermenaces

Peter Stanier, Officier de renseignement sur la cybercriminalité, Réponse aux cybermenaces

Agnese Carlini, Officier de renseignement sur la cybercriminalité, Réponse aux cybermenaces

Dean Watkinson, Officier cyber spécialisé, programme INTERPOL d'appui à l'Union africaine

À PROPOS D'INTERPOL

INTERPOL est l'organisation internationale de police la plus importante au monde. Notre rôle est d'assister les services chargés de l'application de la loi de nos 194 pays membres dans la lutte contre toute forme de criminalité transnationale. Nous nous employons à aider les polices du monde entier à relever les défis – de plus en plus nombreux – de la lutte contre la criminalité au 21ème siècle en leur apportant un appui technique et opérationnel grâce à une infrastructure de pointe. Nos services comprennent des formations ciblées, un soutien spécialisé aux enquêtes, des bases de données spécialisées et un système de communication policière sécurisé.

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.

INTERPOL

INTERPOL Global Complex for Innovation

18 Napier Road

Singapore 258510

WWW.INTERPOL.INT

INTERPOL_HQ

@INTERPOL_Cyber

INTERPOL HQ

INTERPOL