



INTERPOL

# RAPPORT D'ÉVALUATION DES CYBERMENACES EN AFRIQUE

PRÉSENTATION DES PRINCIPALES CYBERMENACES PAR LE  
DESK AFRICAIN POUR LES OPÉRATIONS DE LUTTE CONTRE LA  
CYBERCRIMINALITÉ



Mars 2023

## TABLE DES MATIÈRES

<b>DÉCHARGE DE RESPONSABILITÉ</b>	<b>2</b>
<b>AVANT-PROPOS</b>	<b>3</b>
<b>AVANT-PROPOS</b>	<b>5</b>
<b>ABRÉVIATIONS ET ACRONYMES</b>	<b>7</b>
<b>REMERCIEMENTS</b>	<b>8</b>
<b>RÉSUMÉ</b>	<b>9</b>
<b>1. ÉTAT DU DÉVELOPPEMENT NUMÉRIQUE DANS LA RÉGION AFRICAINE</b>	<b>11</b>
<b>2. PRÉSENTATION DES PRINCIPALES CYBERMENACES EN AFRIQUE : 2022</b>	<b>13</b>
2.1 Escroqueries aux faux ordres de virement	14
2.2 Hameçonnage	16
2.3 Rançongiciels	19
2.4 Chevaux de Troie bancaires et voleurs d'informations	22
2.5 Escroqueries en ligne et extorsion	23
2.6 Logiciels criminels en tant que service	26
<b>3. BRÈVE PRÉSENTATION DES CAPACITÉS EN MATIÈRE DE CYBERCRIMINALITÉ DANS LA RÉGION AFRICAINE</b>	<b>28</b>
<b>4. MARCHE À SUIVRE : ACTION PROACTIVE FACE À L'ÉVOLUTION DES CYBERMENACES DANS LA RÉGION AFRICAINE</b>	<b>30</b>
<b>5. CYCLE ANNUEL DE PLANIFICATION DU DESK AFRICAINE POUR LES OPÉRATIONS DE LUTTE CONTRE LA CYBERCRIMINALITÉ</b>	<b>31</b>

### **DÉCHARGE DE RESPONSABILITÉ**

Les désignations employées dans le présent document et la présentation des données qui y figurent n'impliquent, de la part d'INTERPOL, aucune prise de position quant au statut juridique de tel ou tel pays, territoire, ville ou zone, ou de ses autorités, ni quant au tracé de ses frontières ou limites.

La mention de groupes de pays vise uniquement des fins statistiques ou analytiques et n'exprime pas nécessairement une opinion concernant un pays ou une région en particulier.

La mention de noms de société et de produits ou procédés commerciaux n'implique pas qu'INTERPOL en fasse la promotion, et l'absence de mention d'une société ou d'un produit/procédé commercial ne traduit en aucun cas un avis défavorable à son égard.

INTERPOL a pris toutes les dispositions nécessaires pour vérifier les informations contenues dans la présente publication. Ce contenu est toutefois diffusé sans aucune garantie, expresse ou implicite. La responsabilité de l'interprétation et de l'utilisation dudit contenu incombe au lecteur. INTERPOL ne saurait en aucun cas être tenu pour responsable des préjudices subis du fait de son utilisation.

INTERPOL ne peut garantir que les informations figurant dans le présent document demeureront exactes, et décline toute responsabilité quant au contenu des sites Web externes qui y seraient mentionnés.

INTERPOL se réserve le droit de modifier, de limiter ou de supprimer le contenu de la présente publication.

## AVANT-PROPOS

De nos jours, les technologies sont un aspect incontournable de notre vie, et c'est d'autant plus vrai pour Internet, qui occupe une place centrale dans nos activités professionnelles et personnelles. Il nous permet de contrôler les infrastructures critiques, de réaliser des opérations financières de manière sûre et efficace, de maintenir le contact avec les amis et la famille, d'acheter facilement et rapidement en ligne, mais aussi de se divertir en regardant des vidéos ou en jouant à des jeux. Outre ses nombreuses applications, Internet nous donne un accès sans précédent à des informations qui étaient auparavant hors de portée. Il permet de connecter des personnes aux quatre coins du monde et simplifie le recueil de données et d'informations à des fins de recherche. Il nous permet même d'explorer des univers virtuels qui défient les lois du monde physique. Au vu de tous ces avantages, il n'est pas étonnant qu'Internet soit aujourd'hui omniprésent dans notre vie quotidienne.

L'émergence des nouvelles technologies a également favorisé l'essor de la cybercriminalité ces dernières années. Les cybercriminels affinent sans cesse leurs techniques pour exploiter les nouvelles vulnérabilités, ce qui représente un risque accru pour les personnes et les organisations à l'échelle mondiale. La cybercriminalité d'aujourd'hui est sans commune mesure avec ce qu'elle était hier : les vecteurs d'attaque sont désormais plus complexes, à l'instar des attaques par déni de service distribué (DDoS), des tentatives de hameçonnage, des campagnes de logiciels malveillants, des attaques par rançongiciel et d'autres activités malveillantes susceptibles de causer un préjudice majeur et d'avoir de graves conséquences pour les organisations et les populations.

Il va sans dire que le contexte des menaces évolue en permanence et que de nouvelles formes hybrides de cybercriminalité émergent chaque jour ; il est donc impératif pour les organisations du monde entier de rester vigilant vis-à-vis de ces menaces, en actualisant les protocoles et dispositifs de sécurité en conséquence. En 2023 et au-delà, il sera primordial pour les entreprises, grandes comme petites, d'adopter des solutions globales de cybersécurité qui leur permettront de se protéger contre la multitude de formes traditionnelles de cyberattaques et les nouvelles méthodes hybrides imaginées par des individus malveillants à travers le monde.

Dans le cadre de sa mission de réduction de l'incidence de la cybercriminalité et de protection des populations pour un monde plus sûr, la Direction de la Cybercriminalité d'INTERPOL concentre ses activités sur la prévention, la détection, l'enquête et la perturbation de la cybercriminalité. Pour ce faire, et en vue d'apporter un soutien accru aux pays membres en matière de compréhension des cybermenaces à l'échelle nationale, régionale et mondiale, il convient de recueillir, de traiter, d'analyser et d'évaluer des données et informations sur la cybercriminalité.

Dans cette optique, j'ai l'honneur de vous présenter la deuxième édition du Rapport d'évaluation des cybermenaces en Afrique, rédigé par le Desk africain pour les opérations de lutte contre la cybercriminalité (le « Desk africain »).

Ce rapport contient une analyse approfondie et des informations sur le contexte actuel des cybermenaces dans les pays membres de la région africaine. Les méthodes utilisées par les criminels pour exploiter les vulnérabilités des réseaux et systèmes s'adaptent au gré des évolutions technologiques. Ces dernières années, les pays africains ont constaté une hausse des cyberattaques ciblant les infrastructures critiques, les établissements financiers et d'autres organisations, qui dépendent de plus en plus des services numériques.

Il nous faut admettre que la coopération internationale entre les services chargés de l'application de la loi est une composante essentielle de n'importe quelle stratégie de lutte contre la cybercriminalité. Étant donné que les cybercriminels sont de plus en plus habiles et organisés, une action coordonnée à l'échelle mondiale est nécessaire pour neutraliser efficacement ces menaces.

En collaboration avec nos 195 pays membres et via le recours à des méthodes coordonnées aux niveaux régional et national, nous pouvons améliorer les résultats d'enquête en facilitant l'échange de

renseignements sur les nouvelles menaces, en partageant de bonnes pratiques relatives aux techniques d'enquête et en exploitant pleinement les technologies aux fins du renforcement des capacités.

Par ailleurs, les opérations conjointes doivent être encouragées dans la plus large mesure possible, car elles contribuent à instaurer un climat de confiance entre les pays membres participants, tout en leur donnant l'occasion de bénéficier de l'expérience de leurs homologues en matière de lutte contre des menaces similaires.

Il est également essentiel que les services chargés de l'application de la loi collaborent étroitement avec les organisations du secteur privé, qui détiennent généralement des renseignements précieux sur les nouvelles cybermenaces, proposent des programmes de formation destinés au personnel et partagent une expertise technique dont les organismes publics ne disposent pas toujours. La relation avec le secteur privé permet aux services chargés de l'application de la loi de tirer parti des bases de données et des pouvoirs législatifs pour réagir rapidement aux menaces avant qu'elles n'entraînent un préjudice ou des conséquences majeures.

Dans l'optique de protéger les économies numériques et les populations de la région africaine, le présent rapport expose en outre des stratégies et une marche à suivre pour la région.

Si les cyberinfractions persistantes avancées (CPA), telles que les rançongiciels, le hameçonnage, les chevaux de Troie bancaires et les voleurs d'informations, sont principalement ciblées par le présent rapport, celui-ci contient également une analyse des diverses formes d'escroquerie et de fraude commises à l'aide d'Internet. En effet, dès que ce type d'infractions a été détecté, le Desk africain a mené des actions sur le terrain contre les cybercriminels impliqués via l'élaboration d'un plan d'action intergouvernemental et la coordination d'opérations conjointes (sous les noms de code « Falcon II » et « Delilah »).

L'appui opérationnel accru et l'échange proactif de renseignements renforceront le soutien fourni aux pays membres, en tenant compte des enjeux et besoins spécifiques de la région.

Le présent rapport a pour but d'approfondir la compréhension du contexte régional des cybermenaces afin d'y apporter une réponse prioritaire et ciblée via les réseaux d'INTERPOL.

Nous remercions les pays membres de la région africaine et nos partenaires pour leur solide engagement dans cette entreprise. Nous leur sommes extrêmement reconnaissants pour leur dévouement, leur travail acharné et leur détermination à atteindre cet objectif.



**Craig Jones**  
**Directeur de la Cybercriminalité**  
**INTERPOL**

## AVANT-PROPOS

À la fin des années 1990, les pionniers de l'accès à Internet en Afrique utilisaient des satellites géostationnaires. Seules quelques personnes privilégiées avaient alors accès à Internet. Vingt ans plus tard, tous les pays du continent sont connectés au réseau mondial via des câbles sous-marins ou terrestres, des satellites, voire des drones et des ballons. Dans le sud du Sahara, 25 % de la population dispose d'un accès permanent à Internet, contre 60 % de la population en Afrique du Nord ; en moyenne, seule 50,8 % de la population mondiale est connectée à Internet.

Trente-sept pays africains ont constitué des fonds d'accès universel en vue d'élargir l'accès national à Internet, d'où l'un des taux de croissance de la connectivité les plus élevés du monde enregistré sur le continent africain. Cependant, comme pour toute technologie émergente, l'essor d'Internet s'est accompagné d'une hausse de la cybercriminalité. Les infractions dépendant d'Internet et commises à l'aide d'Internet touchent désormais tous les secteurs d'activité, les nouvelles tendances alliant formes traditionnelles de criminalité et cybercriminalité. À titre d'exemple, les groupes terroristes peuvent recourir aux services de cybercriminels pour lever des fonds via les cybermonnaies, tandis que les réseaux criminels de traite d'êtres humains explorent le Darknet pour développer une expertise en matière de fabrication de faux documents de voyage. En raison de ces évolutions de la criminalité organisée, la lutte contre la cybercriminalité est étroitement liée à la lutte contre toutes les autres formes de criminalité.

Autre constat alarmant : deux ans après la pandémie de COVID-19, les répercussions sont encore sensibles sur le continent africain, notamment à cause de la perte d'emplois, qui a sapé certains secteurs comme l'hôtellerie, le tourisme et l'aviation. Par ailleurs, les méthodes de travail ont évolué depuis la pandémie, certains salariés privilégiant le télétravail, ce qui laisse la porte ouverte à des attaques de type hameçonnage ou FOVI.

La sensibilisation générale à la menace représentée par la cybercriminalité est très concrète sur le continent africain. Les initiatives sous forme de campagnes de sensibilisation ou de conférences régionales et continentales, mais aussi les formations intensives et les programmes de renforcement des capacités, se sont multipliés ces dernières années. Dans le cadre de cette stratégie de lutte contre la cybercriminalité, AFRIPOL a organisé la première session de sa Formation intensive aux enquêtes sur la cybercriminalité, portant notamment sur le hameçonnage, les logiciels malveillants, l'OSINT, le Darknet et les cybermonnaies, du 21 au 23 septembre 2022. Cette première session a rassemblé un total de 136 participants provenant de 22 pays.

AFRIPOL est ravi de sa collaboration avec INTERPOL, qui demeure son principal partenaire, dans le cadre du Programme INTERPOL d'appui à l'Union africaine relativement à AFRIPOL (ISPA). L'année 2022 a été particulièrement fructueuse en la matière, avec la mise en œuvre de nombreux projets : l'opération Cyber Surge Afrique, l'achat de dispositifs de classement numérique SPEKTOR et la formation de sept pays, l'achat de 12 licences CHAINALYSIS et la formation des pays bénéficiaires, mais aussi l'achat d'une vingtaine de licences CyberTOOLBELT et la formation des pays bénéficiaires.

D'autres partenariats, notamment avec la police fédérale allemande via GIZ et le Bureau des Affaires étrangères, du Commonwealth et du Développement du Royaume-Uni, ont permis de mener à bien plusieurs projets, tels que le Réseau d'excellence de la criminalistique et la première Formation intensive à la cybercriminalité. De nombreux projets à grande échelle sont prévus pour 2023, avec le lancement prochain du nouveau centre de données et des bases de données de police scientifique d'AFRIPOL, ainsi que la création d'une unité d'analyse criminelle.

Plus nous progressons dans la lutte contre la cybercriminalité, plus nous nous rendons compte que cette lutte coûte cher et qu'elle nécessite la mise en commun des ressources. Les disparités sont significatives entre les pays africains. Certains disposent d'experts chevronnés et de laboratoires dotés d'outils modernes, tandis que d'autres en sont aux prémices de l'élaboration des cadres législatifs et juridiques fondamentaux en matière de lutte contre la cybercriminalité. Le principe sacré de solidarité qui règne au sein de l'Union africaine appelle une approche globale du problème et des progrès au bénéfice de tous.

Dorénavant, AFRIPOL articule la composante opérationnelle de sa stratégie de lutte contre la cybercriminalité autour des trois axes ci-après:

1. Formation à l'aide de technologies libres et gratuites lorsque le coût des licences payantes empêche les unités de lutte contre la cybercriminalité d'intervenir rapidement.
2. Création d'un fonds pour la lutte contre la cybercriminalité alimenté par les partenaires du secteur pour financer l'achat commun de licences et de matériel en vue de réduire les coûts et la logistique.
3. Renforcement de la collaboration avec le secteur privé dans le but d'harmoniser et de normaliser les procédures et technologies, ainsi qu'aux fins du recueil de renseignements à travers le continent.

L'Afrique rattrape rapidement son retard en termes de connectivité, une arme à double tranchant qui crée à la fois des opportunités de développement et des menaces pour la sécurité des personnes et des biens. Il est en outre évident que la puissance d'Internet permet de s'affranchir des frontières. Une cyberattaque lancée depuis l'Afrique peut atteindre une cible à l'autre bout du monde, c'est pourquoi nous devons mener des actions conjointes de lutte contre le fléau mondial de la cybercriminalité. Le renforcement des capacités de défense et de lutte est nécessaire entre les pays africains et le reste du monde. Pour ce faire, il convient d'harmoniser les procédures, technologies et programmes de formation à l'échelle mondiale.

Enfin, nous espérons que l'année 2023 marquera la réalisation de nos objectifs et une meilleure coordination des actions menées par les services chargés de l'application de la loi.



**Ambassador Jalel CHELBA**  
**Directeur exécutif par intérim,**  
**AFRIPOL**

## ABRÉVIATIONS ET ACRONYMES

<b>AFJOC</b>	Opération conjointe de lutte contre la cybercriminalité en Afrique
<b>CERT</b>	Équipe d'intervention informatique d'urgence
<b>CMII</b>	Complexe mondial INTERPOL pour l'innovation
<b>DDoS</b>	Déni de service distribué
<b>DNS</b>	Système de noms de domaine
<b>FBI</b>	Federal Bureau of Investigation
<b>FOVI</b>	Escroquerie aux faux ordres de virement
<b>HTTPS</b>	Protocole de transfert hypertexte sécurisé
<b>IIC</b>	Infrastructure d'information critique
<b>IP</b>	Protocole Internet
<b>IRC</b>	Internet Relay Chat
<b>OSINT</b>	Renseignement de sources ouvertes
<b>P2P</b>	Pair à pair
<b>PDV</b>	Point de vente
<b>PME</b>	Petites et moyennes entreprises
<b>PPP</b>	Partenariat public-privé
<b>RAT</b>	Outil de prise de contrôle à distance
<b>SAC</b>	Signalement d'activités cybercriminelles
<b>SCC</b>	Serveur de commande et de contrôle
<b>SSL</b>	Secure Sockets Layer
<b>UE</b>	Union européenne

## REMERCIEMENTS

Le présent rapport d'évaluation a été préparé par le Desk africain pour les opérations de lutte contre la cybercriminalité sous l'égide de l'Opération conjointe de lutte contre la cybercriminalité en Afrique (AFJOC) et avec le financement du Bureau britannique des Affaires étrangères, du Commonwealth et du Développement. Le programme INTERPOL d'appui à l'Union africaine (ISPA) y a également contribué, avec le soutien du ministère fédéral allemand des Affaires étrangères.

Le présent rapport s'appuie sur l'évaluation des informations fournies à INTERPOL par les pays membres concernés et les partenaires privés de l'Organisation, dont Group-IB, Kaspersky, Shadowserver et Trend Micro.



## RÉSUMÉ

Dans un contexte de mondialisation où les économies sont toujours plus interconnectées et les technologies évoluent à un rythme effréné, la menace représentée par la cybercriminalité constitue un enjeu majeur pour les pouvoirs publics, les entreprises et les citoyens. La diversité et la complexité des attaques ont connu une croissance exponentielle ces dernières années, les criminels exploitant de nouvelles méthodes d'infiltration pour accéder à des données confidentielles et des informations sensibles.

Alors que cette tendance se poursuit, les risques de sécurité auxquels les organisations sont exposées sont considérablement accrus et engendrent des coûts incommensurables pour l'économie mondiale. Un article publié par le Centre pour la cybersécurité du Forum économique mondial<sup>1</sup> indique que « près de la moitié des entreprises sont touchées par la criminalité économique, dont la cybercriminalité constitue la plus grave menace ».

La cybercriminalité est désormais un secteur qui représente plusieurs milliards de dollars, et les organisations criminelles traditionnelles sont tentées de transférer leurs activités dans le cyberspace ou de commettre des cyberinfractions à l'aide d'outils sophistiqués et de tactiques évolutives, ce qui signifie que les organisations comme les particuliers doivent adapter leurs dispositifs de sécurité. Les cybercriminels se livrent à des activités telles que l'exploitation de mots de passe faibles, la dissimulation de leur identité via des serveurs proxy, le vol d'informations confidentielles appartenant à des entreprises et organismes publics, l'usurpation d'identité et les attaques par rançongiciel.

Les pouvoirs publics du monde entier sont conscients de la menace représentée par la cybercriminalité et investissent des ressources considérables pour protéger leurs citoyens sur Internet. Les services chargés de l'application de la loi ont développé des tactiques efficaces, telles que le renforcement des capacités, le traçage de l'origine des logiciels malveillants et la définition de bonnes pratiques en matière de cybersécurité pour les organisations. Par ailleurs, de nombreux pays collaborent dans le cadre de mécanismes internationaux, à l'instar du Cadre opérationnel conjoint d'INTERPOL, en vue d'accroître l'échange de renseignements sur la cybercriminalité.

En dépit des initiatives menées par les services chargés de l'application de la loi et les pouvoirs publics à travers le monde, les cybercriminels ont toujours un

temps d'avance. Ils sont connus pour tirer parti des failles de sécurité afin d'accéder à des informations sensibles ou à des actifs financiers, ce qui engendre des pertes de plusieurs milliards de dollars chaque année.

Un bon exemple est l'escroquerie aux faux ordres de virement (FOVI), une forme de cybercriminalité transnationale de plus en plus répandue qui ne requiert pas des compétences très techniques mais qui peut entraîner des pertes financières colossales. Rien qu'aux États-Unis d'Amérique, l'Internet Crime Complaint Center (IC3) a indiqué avoir reçu près de 20 000 plaintes pour escroquerie aux FOVI en 2021, soit des pertes ajustées estimées à environ 2,4 milliards USD.

Le Federal Bureau of Investigation a révélé que les escroqueries aux FOVI avaient engendré des pertes faramineuses de plus de 43 milliards USD à l'échelle mondiale, en hausse de 65 % entre 2019 et 2021, très probablement en raison de la pandémie de COVID-19, qui a contraint de nombreuses personnes à exercer leurs activités professionnelles dans le monde virtuel.

Même sans tenir compte des répercussions de la pandémie de COVID-19, le volume et la persistance de ces cyberattaques ne devraient cesser de croître. Les cybercriminels n'ont aucune limite en termes de partage de ressources et de savoir-faire, ce qui explique en partie leur développement. Dans le même esprit, notre rapprochement grâce à l'échange d'informations et de conseils professionnels constitue probablement notre meilleure arme dans la lutte contre la menace frustrante représentée par la cybercriminalité.

En vue de réduire l'incidence mondiale de la cybercriminalité et de protéger les populations pour un monde plus sûr, les services doivent se tenir informés des nouvelles tendances et développer des solutions innovantes pour y répondre. Une intervention rapide permettra de prévenir les activités criminelles et de dissuader les auteurs potentiels.

Grâce aux données issues des pays membres d'INTERPOL, des partenaires privés et des recherches effectuées par le Desk africain pour les opérations de lutte contre la cybercriminalité, ce rapport 2022 fournit une vision globale des tendances en matière de cybercriminalité dans la région africaine. La liste ci-après recense les principales cybermenaces identifiées dans le rapport, une tendance qui se poursuit actuellement dans la région :

<sup>1</sup> Centre pour la cybersécurité du Forum économique mondial (<https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/>)

- **Les campagnes d'escroquerie aux faux ordres de virement** restent prépondérantes, et ce sont les entreprises qui en paient le prix fort : c'est une activité à faible coût et faible risque, mais particulièrement rentable pour les cybercriminels. Ces derniers sont de plus en plus habiles et utilisent des outils très techniques dans le cadre de leurs activités frauduleuses.
- **Le hameçonnage** est une préoccupation croissante en Afrique, en raison de l'adoption rapide et de l'utilisation des technologies numériques. Plus la population se tourne vers les services et applications en ligne, plus elle est vulnérable aux attaques par hameçonnage.
- **Les attaques par rançongiciel**, qui consistent à cibler les pouvoirs publics, des commerces et des organismes publics, se multiplient. Les infrastructures critiques, dont les secteurs de l'énergie et du transport, sont également dans le viseur des cybercriminels.
- **Les chevaux de Troie bancaires et les voleurs d'informations** représentent une nouvelle menace imminente pour les acheteurs sur Internet et sapent la confiance dans les moyens de paiement en ligne. Il est facile de se procurer différents types de chevaux de Troie et de voleurs d'informations sur des forums clandestins, et donc pour les cybercriminels de lancer leurs campagnes malveillantes. L'évolution des fonctionnalités complique la tâche des services chargés de l'application de la loi lorsqu'il s'agit d'enquêter sur ces infractions.
- **Les escroqueries en ligne** se développent à mesure que l'accès à Internet s'élargit. Cette menace est exacerbée par le peu de maîtrise numérique des victimes, ce qui en fait des cibles faciles pour les cybercriminels, qui les mettent en confiance avec de fausses promesses pour leur soutirer de l'argent.
- **La cyberextorsion** doit être étroitement surveillée : elle va de pair avec la prolifération d'Internet et des technologies mobiles, puisque davantage de personnes sont susceptibles de recevoir des demandes de paiement et de se faire extorquer.
- **Les logiciels criminels en tant que service** gagnent en popularité en Afrique, en raison de leur facilité d'utilisation, de leur prix abordable et de l'absence de conséquences liées à la faiblesse des cadres juridiques en matière de répression de la cybercriminalité. C'est un moyen facile pour les criminels de lancer des

attaques à but lucratif contre des systèmes et entreprises vulnérables avec peu de ressources ou de connaissances techniques.

Il convient également de noter que l'élargissement de l'accès aux technologies s'accompagne d'un risque accru d'être victime de ce type d'infractions, c'est pourquoi il est essentiel que les citoyens et les organisations restent vigilants dans leurs interactions numériques. De plus, les services régionaux chargés de l'application de la loi doivent être dotés des outils et connaissances nécessaires pour repérer, enquêter sur et poursuivre les auteurs de ces actes malveillants, mais aussi collaborer avec des partenaires internationaux, comme INTERPOL, à l'échelle mondiale lorsqu'il y a lieu.

Dans le cadre de sa mission de réduction de l'incidence de la cybercriminalité et de protection des populations pour un monde plus sûr, le Desk africain pour les opérations de lutte contre la cybercriminalité d'INTERPOL vise, dans le cadre du projet AFJOC, à s'appuyer sur cette évaluation des menaces pour mener des actions coordonnées et fondées sur le renseignement contre les cyberinfractions et leurs auteurs dans les pays membres africains.

Les efforts collectifs déployés pour échanger des renseignements et élaborer un cadre opérationnel conjoint dynamiseront les capacités et les moyens régionaux de lutte contre la cybercriminalité. La coopération entre les pouvoirs publics, les services chargés de l'application de la loi, les entreprises privées et les établissements d'enseignement supérieur est primordiale pour exploiter au mieux les recueils de données et les ressources disponibles, qui permettront ensuite d'élaborer des stratégies plus efficaces en matière de lutte contre la cybercriminalité. L'efficacité de ces opérations conjointes a déjà été démontrée lors de la récente opération Cyber Surge Afrique, coordonnée par la Direction de la Cybercriminalité d'INTERPOL et le Programme INTERPOL d'appui à l'Union africaine (ISPA), en collaboration avec AFRIPOL.

Outre l'échange accru de renseignements, INTERPOL vise à renforcer les capacités et les moyens régionaux dont les services chargés de l'application de la loi du continent ont besoin pour enquêter efficacement sur les infractions commises à l'aide des technologies.

As well as improving intelligence sharing, INTERPOL is committed to developing the regional capabilities and capacities law enforcement agencies across the continent need if they are to successfully and efficiently investigate cases involving technology-based crime.

## 1. ÉTAT DU DÉVELOPPEMENT NUMÉRIQUE DANS LA RÉGION AFRICAINE

L'Afrique est une région extrêmement diversifiée, caractérisée tant par des paysages désertiques que par des îles tropicales luxuriantes. Elle compte la deuxième plus grande population mondiale et est l'une des régions les plus variées sur le plan culturel. Elle regorge par ailleurs de ressources naturelles comme le pétrole et le gaz, l'or et les diamants, les minerais d'étain et cuivre, l'uranium, le bauxite, et bien d'autres minéraux. Ces ressources figurent parmi les principaux leviers de la croissance économique en Afrique, aux côtés de secteurs comme l'agroalimentaire, la production industrielle et le tourisme.

L'Afrique dispose d'une multitude de terres arables qui favorisent l'exploitation agricole dans bon nombre de ses pays, un secteur qui représente un quart du PIB de ces derniers.

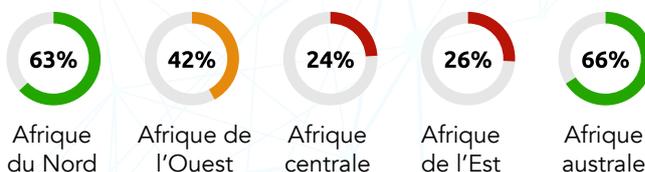


La production industrielle occupe une place de plus en plus importante dans le développement du continent depuis quelques années. L'accent mis sur la production à valeur ajoutée a entraîné une hausse significative des investissements directs étrangers, une création d'emplois et une stimulation de l'économie locale dans de nombreuses zones de la région.

Le PIB cumulé de la région<sup>2</sup> a plus que quintuplé en à peine 20 ans, passant de 695,88 milliards USD en 2002 à 2 980 milliards USD en 2022. La région africaine est l'un des plus grands marchés au monde, et devrait dépasser les 4 000 milliards USD d'ici 2027.

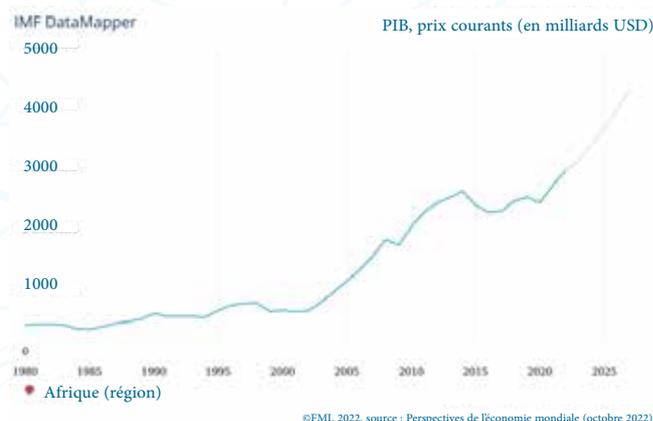
Le taux de pénétration d'Internet en Afrique est relativement élevé par rapport au taux mondial.

D'après le 2022 Global Digital Report<sup>3</sup>, le taux moyen de pénétration d'Internet en Afrique est d'environ 44 %.



Il a connu une augmentation rapide au cours des dernières années et ne semble pas près de ralentir, étant donné que les pays africains investissent massivement dans les infrastructures et l'accès au numérique. Par ailleurs, de nombreux pays déploient actuellement la 5G à l'échelle nationale, ce qui accentue cette hausse.

Il convient également de noter que cette croissance est en grande partie attribuable à l'utilisation de l'Internet mobile (par opposition aux connexions fixes), du fait de sa praticité et de son prix abordable. Les réseaux mobiles sont de plus en plus fiables dans la plupart des pays africains, ce qui permet à la population de rester virtuellement en contact et de bénéficier de services en ligne tels que le commerce électronique et les plateformes de médias sociaux.



En outre, plusieurs gouvernements africains prennent des mesures visant à garantir un accès équitable pour tous aux outils numériques et aux nouvelles opportunités offertes par cet environnement numérique en constante évolution. À titre d'exemple, l'Union africaine a lancé la Stratégie de transformation numérique pour l'Afrique (2020-2030)<sup>4</sup>, dont l'objectif est de fournir une connexion

<sup>2</sup> PIB (actuel) en USD. Source : Fonds monétaire international

<sup>3</sup> 2022 Digital Global Report (www.wearesocial.com)

<sup>4</sup> La Stratégie de transformation numérique pour l'Afrique (2020-2030) (<https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf>)

Internet à tous les citoyens africains d'ici 2023, mais également de développer des compétences numériques inclusives et des ressources humaines dans différents domaines comme le codage, la programmation, l'analyse, la sécurité, les chaînes de blocs, l'apprentissage automatique, l'intelligence artificielle, la robotique, l'ingénierie, l'innovation, l'entrepreneuriat, ou encore les politiques et la réglementation applicables aux technologies.

Par ailleurs, le taux moyen de pénétration des médias sociaux dans la région africaine est d'environ 27 %, avec davantage d'utilisateurs actifs en Afrique du Nord (56 %) et en Afrique australe (45 %).

L'Afrique connaît actuellement une croissance et un développement sans précédent dans le secteur des technologies numériques, en particulier s'agissant des technologies de la finance et du commerce électronique. Cet essor accroît la demande de services Internet et haut débit, ce qui en fait l'un des marchés les plus concurrentiels au monde. Une multitude d'investisseurs du monde entier rivalisent pour exploiter cette opportunité, mais la dépendance accrue aux infrastructures en ligne s'accompagne de diverses menaces de sécurité pouvant entraîner des problèmes majeurs.

La transformation numérique de l'Afrique est un phénomène en expansion qui permet à de nombreux pays du continent de tirer parti des évolutions des technologies modernes pour stimuler leur croissance économique et élargir l'accès aux services essentiels. Le développement des technologies numériques à travers le continent pousse progressivement les pays africains à les adopter et à les intégrer dans leur économie. Ce processus de transformation numérique est favorisé par plusieurs facteurs, dont la disponibilité accrue des données et informations, un meilleur accès à Internet, l'émergence de start-ups et organisations innovantes, le perfectionnement des infrastructures de communication et de commerce, ou encore les initiatives publiques visant à promouvoir l'investissement dans le numérique.

Ces dernières années, bon nombre de pays africains ont enregistré des progrès notables en matière de transformation numérique. L'Éthiopie,

par exemple, a mis en œuvre des stratégies axées sur les technologies<sup>5</sup>, à l'instar du National Rural Land Administration Information System (NRLAIS), qui a permis de gagner en efficacité dans le secteur agricole. Au Kenya, des sociétés de technologie comme Microsoft aident les agriculteurs à utiliser les données pour adopter des pratiques agricoles plus efficaces. Le Rwanda s'est également lancé dans la transformation numérique via le développement d'initiatives dans le cadre de son Smart City Rwanda Masterplan.<sup>6</sup>

5 Digital Ethiopia 2025 (<https://www.pmo.gov.et/media/other/b2329861-f9d7-4c4b-9f05-d5bc2c8b33b6.pdf>)

6 Smart City Rwanda Masterplan ([https://www.minict.gov.rw/fileadmin/user\\_upload/minict\\_user\\_upload/Documents/Strategies/Smart\\_City\\_Rwanda\\_Masterplan.pdf](https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Strategies/Smart_City_Rwanda_Masterplan.pdf))

## 2. PRÉSENTATION DES PRINCIPALES CYBERMENACES EN AFRIQUE : 2022

Grâce aux données issues des pays membres d'INTERPOL dans la région africaine, des partenaires privés et des recherches effectuées par le Desk africain pour les opérations de lutte contre la cybercriminalité, cette partie comprend une analyse approfondie des menaces et des tendances en matière de cybercriminalité, ainsi que de leurs motivations sous-jacentes.

Le Desk africain pour les opérations de lutte contre la cybercriminalité a identifié certaines des principales cybermenaces en 2022, une tendance qui se poursuit actuellement dans les pays membres de la région.

### Escroqueries aux faux ordres de virement (FOVI)

Les escroqueries aux faux ordres de virement sont une forme de cyberattaque qui consiste, pour des individus malveillants, à obtenir un accès non autorisé au compte de messagerie d'une organisation et à l'utiliser pour envoyer des messages frauduleux à ses partenaires commerciaux dans un but lucratif. Ces courriels contiennent généralement des liens ou pièces jointes malveillants qui, lorsque l'on clique dessus, installent un logiciel malveillant sur l'appareil du destinataire ou permettent à l'expéditeur d'accéder à des informations confidentielles. Outre l'envoi de courriels, les cybercriminels peuvent manipuler les chaînes de courriel existantes et supprimer des messages importants comme des demandes de paiement contenant des coordonnées bancaires. Les escroqueries aux faux ordres de virement peuvent engendrer des pertes financières considérables et ternir la réputation d'une organisation.

### Hameçonnage

Le hameçonnage est une forme de cyberattaque qui consiste, pour des individus malveillants, à voler des informations sensibles telles que les noms d'utilisateur, les mots de passe et les coordonnées bancaires appartenant à des victimes non averties. Les hameçonneurs utilisent généralement de faux comptes de messagerie ou sites Internet d'apparence authentique pour inciter les victimes à communiquer des informations personnelles. Ils peuvent également avoir recours à l'ingénierie sociale sous forme d'usurpation d'identité et d'attaques par logiciel malveillant pour accéder à des données confidentielles. Les attaques par

hameçonnage peuvent causer un préjudice financier majeur et faciliter l'usurpation d'identité.

### Rançongiciels

Les rançongiciels sont une forme malveillante de logiciels qui bloquent l'accès des utilisateurs à leurs propres données, systèmes et appareils en cryptant leurs fichiers. Une fois le cryptage terminé, les victimes reçoivent un message les informant qu'elles doivent s'acquitter d'une certaine somme (souvent en bitcoin ou dans une autre cybermonnaie) pour que leurs fichiers soient décryptés et qu'elles puissent à nouveau y accéder. Ce type d'attaque gagne en popularité chez les cybercriminels grâce à sa capacité à générer rapidement des bénéfices juteux avec peu de ressources : dans la plupart des cas, un seul courriel suffit pour mener à bien une attaque par rançongiciel. Les rançongiciels peuvent également être propagés via des publicités malveillantes sur les sites Internet et les médias sociaux, mais aussi via des téléchargements malveillants.

### Chevaux de Troie bancaires et voleurs d'informations

Les chevaux de Troie bancaires et les voleurs d'informations sont des logiciels malveillants destinés à voler des informations sensibles telles que les noms d'utilisateur, les mots de passe et les données financières appartenant à des victimes non averties. Ces chevaux de Troie peuvent être installés via des courriels de hameçonnage, des sites Internet malveillants, des téléchargements furtifs ou d'autres moyens. Une fois le cheval de Troie installé sur l'ordinateur de la victime, il tente d'accéder à ses comptes bancaires en ligne en enregistrant la frappe ou en volant les identifiants de connexion. Il peut également modifier les pages qui s'affichent dans le navigateur afin de rediriger les éventuels transferts de fonds vers le compte du criminel au lieu de celui du destinataire prévu. Les chevaux de Troie bancaires sont souvent combinés à d'autres logiciels malveillants comme des logiciels espions et des rootkits en vue d'accélérer leur propagation à travers un réseau ou un système.

Les chevaux de Troie bancaires sont de plus en plus complexes et recourent à des techniques avancées de type « man-in-the-browser », qui permettent aux cybercriminels de manipuler des opérations sans être repérés.

## Escroqueries en ligne

Les escroqueries en ligne sont la forme la plus courante et la plus dangereuse d'escroquerie, dont la dimension est internationale. Les escroqueries en ligne désignent tout type d'infraction frauduleuse commise via un ordinateur ou à l'aide de données informatiques.

## Cyberextorsion

La cyberextorsion consiste, pour un criminel, à utiliser des techniques numériques pour menacer des victimes ou leur extorquer de l'argent et/ou d'autres actifs. En règle générale, le cybercriminel menace de révéler des informations personnelles gênantes, de supprimer des données importantes, de saboter des systèmes et réseaux, ou encore de lancer une attaque par déni de service distribué (DDoS).

## Logiciels criminels en tant que service

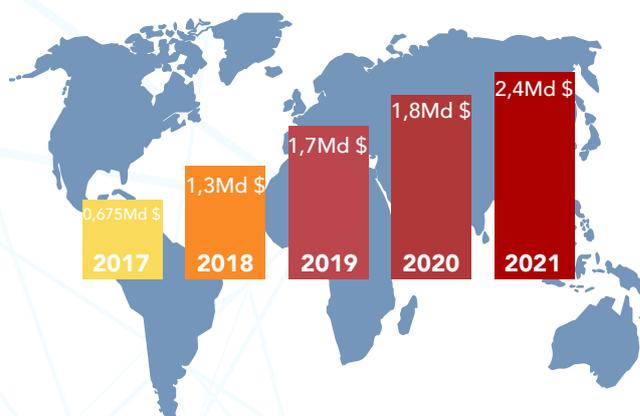
Les logiciels criminels en tant que service, ou CaaS, désignent un programme ou un ensemble de programmes informatiques destinés à faciliter les activités illégales en ligne. Les logiciels espions, les kits de hameçonnage, les pirates de navigateur, les enregistreurs de frappe et bien d'autres outils malveillants sont mis à la disposition des cybercriminels sous forme de CaaS.

### 2.1 Escroqueries aux faux ordres de virement

Pour la septième année consécutive, les escroqueries aux faux ordres de virement (FOVI) constituent la cybermenace la plus dévastatrice d'un point de vue financier à l'échelle mondiale. Rien que l'année dernière, les entreprises américaines ont enregistré des pertes faramineuses de 2,4 milliards USD<sup>7</sup> à cause de ces attaques, soit un bond de 28 % et de plus d'un demi-milliard de dollars par rapport à 2020. Ces chiffres alarmants nous rappellent à quel point les escroqueries aux FOVI peuvent être puissantes et préjudiciables pour des entreprises de toute taille.

Outre des pertes financières considérables, les escroqueries aux FOVI peuvent ternir la réputation d'une organisation si ses clients apprennent qu'elle a été victime de ce type d'activités malveillantes.

### PERTES LIÉES AUX ESCROQUERIES AUX FOVI POUR LES ENTREPRISES AMÉRICAINES



La plupart des auteurs d'escroqueries aux FOVI sont implantés en Afrique de l'Ouest, mais malheureusement pour les victimes, leurs manœuvres s'affranchissent des frontières. Ces criminels sont généralement en lien avec de plus vastes réseaux criminels à l'échelle mondiale, ce qui leur permet de cibler un grand nombre de victimes aux quatre coins du monde. Fait effrayant, les auteurs d'escroqueries aux FOVI se livrent également à une multitude d'autres cyberinfractions.

Ces escrocs sont de plus en plus habiles et ont développé des méthodes pour éviter d'être repérés par les services chargés de l'application de la loi : ils utilisent notamment plusieurs comptes de messagerie électronique et font transiter les fonds par des comptes bancaires internationaux et des sociétés-écrans. Ils utilisent également des réseaux de communication cryptés comme les applications de messagerie instantanée ou les forums du Darknet pour dissimuler leurs activités, ce qui complique encore la tâche des services chargés de l'application de la loi pour retrouver leur trace, d'autant qu'ils se trouvent parfois dans plusieurs pays ou juridictions.

De plus, certains escrocs s'associent à des mules financières qui les aident à blanchir de l'argent via des sociétés-écrans et des comptes bancaires offshore. Cela leur permet de préserver leur anonymat et les met hors de portée des autorités.

En réponse à la forte concentration d'auteurs d'escroqueries aux FOVI détectée dans la région nigériane, le Desk africain pour les opérations

<sup>7</sup> Federal Bureau of Investigation Internet Crime Report 2021 ([https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf))

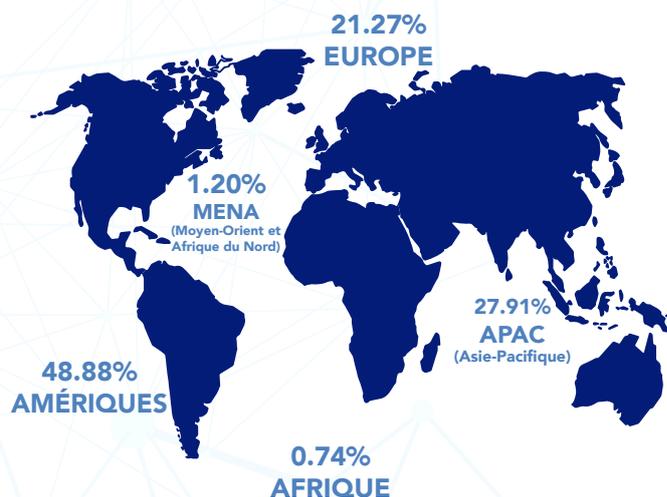
de lutte contre la cybercriminalité d'INTERPOL, assisté de ses partenaires privés Group-IB, Palo Alto Networks et Trend Micro ainsi que de la police nigériane (NPF), a mené avec succès l'opération Delilah<sup>8</sup> en mai 2022. Le but de cette opération était de désorganiser un groupe prolifique d'escroqueries aux FOVI connu sous le nom de « SilverTerrier » ou « TMT » ; elle a donné lieu à l'arrestation du chef d'un groupe cybercriminel transnational.

L'équipe en charge de l'opération Delilah a également identifié les principaux individus directement impliqués dans la commission de ces cyberinfractions, ce qui a permis de limiter fortement leur capacité à poursuivre leurs activités criminelles. Par ailleurs, des éléments de preuve cruciaux ont été recueillis et ont conduit à la détection et la confiscation de fonds volés, mais aussi de documents compromettants et d'appareils numériques utilisés par les membres du réseau criminel.

Cette action proactive a été suivie d'une autre opération baptisée « Killer Bee<sup>9</sup> », étayée par des renseignements issus d'un partenaire du secteur privé, Trend Micro. L'opération, menée par INTERPOL, a donné lieu à l'arrestation de trois auteurs d'escroqueries aux FOVI d'origine nigériane à la suite d'une enquête approfondie diligentée par la Commission de lutte contre la criminalité économique et financière (EFCC) du Nigéria. Ces individus auraient utilisé un cheval de Troie contenant un outil de prise de contrôle à distance (RAT) pour détourner des opérations financières et voler des informations confidentielles sur les connexions à des sociétés, notamment pétrolières et gazières, en Asie du Sud-Est, au Moyen-Orient et en Afrique du Nord.

Le succès rencontré par les opérations Delilah et Killer Bee en matière de désorganisation des escroqueries aux FOVI au Nigéria montre à quel point il est primordial que les organisations internationales œuvrant dans le domaine de l'application de la loi telles qu'INTERPOL et les services nationaux chargés de l'application de la loi comme la NPF et l'EFCC unissent leurs forces pour lutter efficacement contre les réseaux criminels

organisés à travers le pays. Ces actions communes fournissent un appui supplémentaire en vue de démanteler les réseaux cybercriminels complexes, et ainsi, une protection renforcée contre diverses formes d'escroqueries et d'activités malveillantes en ligne pour les citoyens.



#### TENTATIVES D'ESCROQUERIE AUX FOVI PAR RÉGION (2021 - MAI 2022).

SOURCE: TREND MICRO

Trend Micro a par ailleurs indiqué que les cybercriminels ciblaient de plus en plus d'autres régions, notamment celles qui concentrent davantage de cibles de grande importance, où les répercussions économiques sont plus fortes.

La région africaine est également victime d'escroqueries aux FOVI depuis quelques années, l'augmentation constante des cyberattaques y causant des pertes financières et perturbant les activités économiques.

Bien que les pays africains n'aient été concernés que par 0,75 % des tentatives d'escroquerie aux FOVI à l'échelle mondiale entre 2021 et mai 2022, les données issues de Trend Micro révèlent que l'Afrique du Sud a été victime de plus de la moitié des cas d'escroquerie aux FOVI recensés dans la région au cours de la même période.

La menace représentée par les escroqueries aux FOVI est exacerbée dans la région africaine, en

8 Le chef présumé d'un groupe cybercriminel arrêté au Nigéria, mai 2022 (<https://www.interpol.int/News-and-Events/News/2022/Suspected-head-of-cybercrime-gang-arrested-in-Nigeria>)

9 escroquerie en ligne : trois Nigériens arrêtés dans le cadre de l'opération Killer Bee d'INTERPOL, mai 2022 (<https://www.interpol.int/en/News-and-Events/News/2022/Online-scamming-fraud-three-Nigerians-arrested-in-INTERPOL-Operation-Killer-Bee>)

raison de la transition rapide vers une économie toujours plus numérique. L'augmentation constante d'utilisateurs dépendant des technologies pour leurs opérations quotidiennes multiplie les opportunités pour les individus malveillants d'exploiter les organisations vulnérables. Sans compter que de nombreux pays d'Afrique ne disposent pas de mesures de cybersécurité efficaces, ce qui accroît encore le risque d'escroqueries aux FOVI.

Autre facteur alimentant la hausse de ce type de cyberattaque en Afrique : l'absence de pratiques élémentaires de cybersécurité au sein des entreprises exerçant des activités sur le continent. La plupart des organisations n'ont pas adopté de politiques adéquates en matière de gestion des protocoles de contrôle d'accès, des procédures d'authentification ou des normes de chiffrement, ce qui les expose à des cyberattaques via des systèmes non sécurisés et des comptes d'utilisateur associés à des mots de passe faibles. Autrement dit, même si un salarié était en mesure de détecter des courriels frauduleux envoyés par des escrocs, il n'aurait pas la possibilité de se protéger contre la menace (financière ou opérationnelle) qu'ils représentent, puisque les mécanismes de défense adéquats n'ont pas été instaurés dès le départ.

L'une des caractéristiques les plus récurrentes des escroqueries aux FOVI en Afrique est le recours à l'ingénierie sociale : en effet, les escrocs tirent parti de leur maîtrise de la culture locale et de la langue. Ces individus malveillants se font par exemple passer pour une connaissance de leur victime et créent un sentiment d'urgence ou de panique, si bien que la victime satisfait les demandes formulées dans les courriels sans vérifier s'ils sont authentiques.

Les statistiques issues des 22 pays membres de la région africaine révèlent que 399 cas d'escroquerie aux FOVI ont été signalés aux services chargés de l'application de la loi en 2021.

L'évaluation des données relatives aux cas d'escroquerie aux FOVI dans la région africaine permettrait d'obtenir une vision plus précise de la situation. Malheureusement, force est de constater qu'un grand nombre de ces cas ne sont pas signalés dans cette région, ce qui aggrave le problème. L'insuffisance des signalements entrave la capacité des services chargés de l'application de la loi de

poursuivre l'ensemble des criminels impliqués et d'affecter les ressources plus efficacement pour lutter contre cette forme de cybercriminalité.

Il est donc primordial de sensibiliser les entreprises à l'importance de signaler les escroqueries aux FOVI dont elles sont victimes afin que des informations précieuses sur ces activités cybercriminelles puissent être recueillies par les services chargés de l'application de la loi du continent africain, qui pourront ainsi mieux cerner cette tendance criminelle et prendre des mesures pour la combattre.

## 2.2 Hameçonnage

Le hameçonnage est l'une des cybermenaces les plus anciennes et les plus répandues. L'on estime que jusqu'à 90 % des violations de données<sup>10</sup> sont liées à des attaques par hameçonnage réussies, qui constituent donc une source majeure d'identifiants et d'informations volés. Les techniques de hameçonnage sont de plus en plus complexes, les cybercriminels parvenant à cibler leurs victimes avec plus de précision. Ils sont capables de rédiger des messages qui semblent provenir de sources fiables comme des banques, des services publics, voire des amis et des membres de la famille. Ces messages contiennent généralement des liens ou pièces jointes malveillants qui redirigent les victimes vers des sites Internet ou des fichiers intégrant des virus ou des logiciels malveillants.

Outre le vol d'identifiants, le but ultime des attaques par hameçonnage est d'accéder à des données confidentielles telles que des informations financières, des mots de passe, des coordonnées détaillées, etc. Une fois ces données en leur possession, les cybercriminels les utilisent à but lucratif et/ou aux fins d'usurpation d'identité en les vendant sur des cryptomarchés ou en se livrant à d'autres activités malveillantes comme l'extorsion. Le hameçonnage représente ainsi une grave menace, non seulement en raison des éventuelles pertes financières, mais également en raison du préjudice résultant d'autres cyberinfractions facilitées par une attaque réussie.

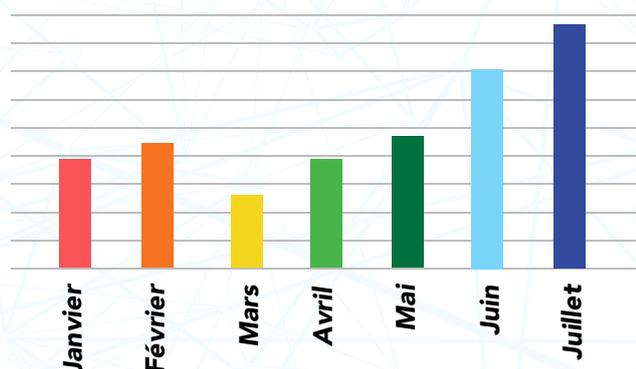
Tandis que les technologies évoluent et que les cybercriminels perfectionnent leurs techniques, le hameçonnage demeure une menace omniprésente pour les organisations comme pour les particuliers.

10 CISCO's 2021 Cybersecurity Threat Trends Report (<https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list>)

Les cybercriminels ont recours à l'ingénierie sociale sous forme d'usurpation d'identité et de tactiques alarmistes pour accroître leurs chances de réussite. De plus, les outils automatiques comme les spambots leur permettent d'envoyer un grand nombre de courriels ou de messages et d'accroître ainsi leurs chances de réussite. La combinaison de tous ces facteurs engendre un degré de risque inégalé en lien avec les attaques par hameçonnage, ce qui en fait l'une des cybermenaces les plus dangereuses à l'heure actuelle.

Entre janvier et juillet 2022, Kaspersky a recensé un nombre alarmant d'outils de hameçonnage (15 769 298) en Afrique. La plupart de ces activités malveillantes sont menées via des courriels ou des pages Internet à l'aide d'une méthode bien connue d'ingénierie sociale appelée « hameçonnage ».

#### Détection d'outils de hameçonnage par Kaspersky entre jan. et juil. 2022



Entre janvier et août 2022, Group-IB a identifié un nombre alarmant d'URL de hameçonnage (1 352 412) dans la région africaine. Il s'agit d'un problème de sécurité majeur, car les attaques par hameçonnage peuvent avoir des conséquences dévastatrices pour les personnes et organisations qu'elles prennent au dépourvu.

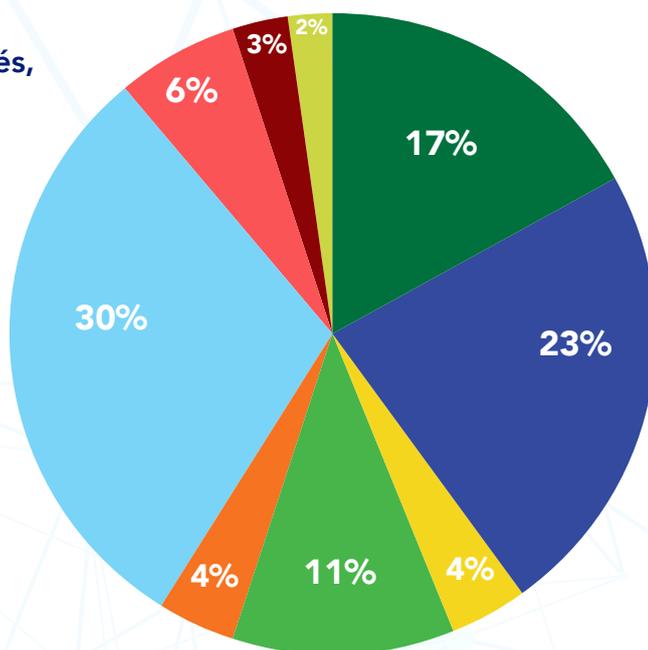
L'une des techniques de hameçonnage les plus courantes en Afrique est celle de l'anniversaire de marque. Les cybercriminels se font passer pour une marque renommée, comme Ethiopian Airlines, et appâtent des personnes non averties en leur promettant un cadeau si elles répondent à une courte enquête ou un questionnaire. Une fois que la personne a renseigné ses coordonnées, elle est invitée à transmettre le message à cinq groupes WhatsApp ou 20 amis pour recevoir sa récompense. En réalité, les escrocs saisissent cette opportunité

pour recueillir des données personnelles et des informations sur l'appareil utilisé par la personne répondant à leur sollicitation sans se douter de rien.

L'escroquerie à l'anniversaire de marque n'est qu'un exemple de la puissance et de l'efficacité des attaques par hameçonnage pour les criminels en quête de bénéfices rapides issus d'activités illicites menées aux dépens de victimes innocentes. Les courriels de hameçonnage sont de plus en plus sophistiqués en termes de format et de contenu, ce qui rend leur détection difficile pour une personne lambda. De plus, les criminels ont recours à l'ingénierie sociale afin que ces courriels paraissent plus authentiques. À titre d'exemple, de nombreux escrocs créent de faux comptes de messagerie en utilisant des noms de domaine similaires à ceux d'entreprises légitimes pour accroître leurs chances de réussite lorsqu'ils ciblent des utilisateurs non avertis. La plupart des victimes pensent alors échanger avec un vrai représentant de l'entreprise, et non un imposteur.

Cette menace est exacerbée par le manque de campagnes de sensibilisation et d'information adressées au grand public. De fait, les citoyens ne sont pas correctement informés sur ce type d'escroquerie et ne disposent pas de ressources ni de conseils pour se protéger contre ces cybermenaces. Le manque de connaissances sur l'hygiène informatique en Afrique rend la population encore plus vulnérable et laisse le champ libre aux auteurs de ces infractions, qui peuvent ainsi lancer des attaques par hameçonnage sans être repérés par les autorités.

**Secteurs les plus touchés,  
T3 2022**



**30% Autres**

**23% Établissements financiers**

**17% SaaS / messageries électroniques**

**11% Médias sociaux**

**6% Logistique/transport**

**4% Commerce (dont électronique)**

**4% Paiement**

**3% Télécommunications**

**2% Cybermonnaies**

Le dernier rapport<sup>11</sup> publié par l'Anti-Phishing Working Group révèle que le secteur financier, auquel appartiennent les banques, est la principale cible du hameçonnage, puisqu'il est victime de plus de 23 % des attaques. Le nombre d'attaques ciblant les fournisseurs de messageries électroniques et de logiciels en tant que service (SaaS) reste stable, tandis que celles ciblant les commerces (physiques et en ligne) ont chuté, passant de 14,6 % à 4 %.

La prolifération des attaques par hameçonnage s'explique par la relative facilité avec laquelle un individu peut se livrer à ce type d'activité criminelle. En effet, le hameçonnage en tant que service (PaaS) est accessible sur les cryptomarchés. Pour la modique somme de 20 USD, n'importe qui peut acheter un kit de hameçonnage, fourni avec tout le matériel nécessaire au lancement d'une attaque. Des tutoriels vidéo expliquent également comment monter et utiliser le kit. Il existe en outre des options de service après-vente comprenant des mises à jour régulières afin d'éviter que les courriels de hameçonnage des criminels ne soient détectés par les solutions de sécurité Internet modernes. Même sans connaissances techniques, ces individus

malveillants peuvent lancer des attaques par hameçonnage avec peu de ressources.

Dans le cadre de ses recherches, Group-IB a identifié une publication sur un forum XSS dans laquelle un cybercriminel faisait la publicité de pages de hameçonnage ciblant des banques. Parmi ces banques figurait Banco BIC, une banque d'origine portugaise et angolaise qui possède de nombreuses succursales à travers le monde. La publication se targuait de vendre, à un prix modique, des pages de hameçonnage permettant d'accéder à des comptes d'utilisateur.

Ces faibles barrières à l'entrée ont entraîné une hausse des activités de hameçonnage ces dernières années. Les kits contiennent généralement des bribes de code et des scripts écrits par des développeurs chevronnés qui permettent aux utilisateurs d'héberger leurs sites Internet sans même savoir comment cela fonctionne. Ils comprennent également des outils anti-détection et des modèles prêts à l'emploi pour créer des courriels efficaces, capables de contourner le filtrage du courrier indésirable en vue d'arriver

<sup>11</sup> APWG Phishing Activity Trends Report 3rd Quarter 2022 (<https://apwg.org/trendsreports/>)

dans la boîte de réception des victimes sans être détectés. Ainsi, les individus se livrant à ce type d'activité criminelle n'ont même pas besoin de posséder des compétences élémentaires de codage ou un quelconque savoir-faire technique ; n'importe qui ayant accès au marché noir et disposant de quelques dollars en poche peut se transformer en cybercriminel professionnel comme par magie.

Bien que de nombreuses attaques par hameçonnage soient détectées dans la région africaine, le nombre de signalements aux services chargés de l'application de la loi est bien inférieur. Dans une vingtaine de pays d'Afrique, seuls 2 087 cas ont été signalés ; cet écart est attribuable à plusieurs facteurs, dont la mauvaise classification des affaires et un manque d'information du grand public sur la manière de signaler ce type d'infractions.

Sur les 42 pays africains interrogés, 24 ont indiqué ne pas encore avoir créé de plateforme en ligne ou de mécanisme de signalement des cyberinfractions à la disposition du grand public. Ces lacunes entravent la capacité des services chargés de l'application de la loi à détecter les cyberattaques et à intervenir efficacement. De fait, ces incidents sont souvent insuffisamment signalés, voire totalement ignorés.

### 2.3 Rançongiciels

Les attaques par rançongiciel s'inscrivent en forte hausse depuis quelques années, et elles sont désormais considérées comme l'une des plus graves menaces pour les organisations de toute taille à travers le monde. Les cybercriminels utilisent ces logiciels malveillants pour prendre le contrôle des systèmes critiques d'une organisation et crypter les données qu'ils contiennent, puis ils demandent à se faire payer pour rétablir l'accès. Ces attaques peuvent coûter très cher aux entreprises, car les pertes financières liées à l'indisponibilité des systèmes et aux mesures de rétablissement s'accumulent rapidement.

Les attaques par rançongiciel ne semblent pas près de ralentir, et les coûts y afférents devraient augmenter en 2023. Cybersecurity Ventures<sup>12</sup>, l'un des chefs de file de la recherche et de l'édition dans

le domaine de la cybersécurité, estime qu'à l'échelle mondiale, le coût des attaques par rançongiciel atteindra 265 milliards USD d'ici 2031.

Les entreprises victimes de ces attaques risquent également une atteinte majeure à leur réputation, puisque les données de leurs clients peuvent être rendues publiques ou volées dans le cadre de ces incidents, compromettant ainsi leur fiabilité aux yeux des clients et d'autres parties prenantes.

**3x** Augmentation du nombre de rançons payées de 1 M USD ou plus

**21%** de rançons payées de moins de 10 000 USD

**812 360 USD** Montant moyen des rançons (hors valeurs aberrantes)

**PRODUCTION, SERVICES DE DISTRIBUTION** Montant moyen des rançons le plus élevé (2 M USD)

**SANTÉ** Montant moyen des rançons le plus bas (197 000 USD)

SOURCE : THE STATE OF RANSOMWARE 2022 (SOPHOS)

D'après le 2022 Cost of a Data Breach Report<sup>13</sup> d'IBM, le coût total moyen d'une attaque par rançongiciel, qui s'élève à pas moins de 4,54 millions USD, est bien supérieur à celui d'une violation de données, atteignant tout de même 4,35 millions USD. La part de violations causées par des rançongiciels a augmenté de 41 % l'année dernière, et il a fallu 49 jours de plus que la moyenne pour les détecter et les maîtriser.

12 Global Ransomware Damage Costs (<https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/13>)

13 Cost of a Data Breach Report 2022 (<https://www.ibm.com/reports/data-breach>)

Ces données sont confirmées par The State of Ransomware 2022<sup>14</sup> de Sophos, qui indique que les organisations de taille moyenne paient des rançons encore plus élevées, de 812 360 USD en moyenne par attaque. Ces coûts peuvent être ventilés par poste, tel que l'indisponibilité et le temps nécessaire à la mise en œuvre des mesures d'atténuation, le coût des appareils (remplacement ou réparation du matériel touché), le coût des réseaux (rétablissement des réseaux ou services), les occasions manquées en raison du retard pris dans les activités, et le paiement de la rançon par les organisations, le cas échéant.

Le Trésor américain<sup>15</sup> a par ailleurs indiqué que les banques américaines avaient traité près de 1,2 milliard USD de paiements de rançon en 2021, soit bien plus que ce que la plupart des pirates informatiques auraient pu imaginer lorsqu'ils ont développé les premiers rançongiciels il y a plusieurs décennies.

Avec de telles perspectives financières, il est probable que l'essor des rançongiciels se poursuive, à moins que des mesures fortes ne soient prises pour les combattre, car ils nécessitent peu de ressources et sont largement automatisés, le risque de se faire prendre est faible et les bénéfices sont juteux.

D'après Shadowserver, les données compilées à partir de sites de fuite de données entre janvier et septembre 2022 révèlent que les victimes africaines sont ciblées par un vaste éventail de familles de rançongiciels. Au cours de cette période, la principale famille de rançongiciels identifiée était Lockbit 2.0, représentant environ 38,8 % des attaques détectées en Afrique. Elle était suivie de près par Pysa (14,3 %) et Lockbit 3.0 (8,2 %). Parmi les autres familles de rançongiciels identifiées sur la période, citons Conti, HiveLeaks, Midas et BlackByte (4,1 % pour chaque).

Les répercussions d'autres programmes malveillants ne doivent toutefois pas être sousestimées. Toutes ces menaces sont susceptibles de perturber fortement les activités économiques via le cryptage de données ou systèmes critiques, donnant lieu au paiement d'une grosse rançon ou

à une indisponibilité prolongée, le temps que les organisations parviennent à récupérer les fichiers infectés. De plus, la prolifération des rançongiciels a entraîné une hausse alarmante des cyberinfractions à but lucratif dans la région africaine.

Shadowserver a également indiqué que l'Afrique du Sud était le pays le plus touché par les attaques par rançongiciel, à hauteur de 42 % des attaques détectées. S'ensuivent le Maroc (8 %), puis le Botswana et l'Égypte (6 % respectivement). La Tanzanie et le Kenya enregistrent chacun 4 % des attaques par rançongiciel détectées. Un tel nombre d'activités malveillantes en Afrique du Sud est préoccupant, car il suggère que le nombre d'attaques par rançongiciel non détectées dans le pays est encore plus élevé.

La plupart de ces activités malveillantes sont probablement facilitées par des systèmes obsolètes et des solutions de sécurité inefficaces, qui créent des failles à exploiter par les cybercriminels. L'absence de réglementation et de législation relatives à la cybercriminalité contribue également à la multiplication des attaques par rançongiciel dans les pays de la région. Sans règles ni directives claires en matière de protection contre ces menaces, bon nombre d'organisations sont à la merci des cybercriminels.

D'après Trend Micro, les attaques par rançongiciel ne représentent que 1,4 % des cyberinfractions détectées à travers le monde entre janvier et juillet 2022. Néanmoins, la menace qu'elles représentent dans la région africaine est bien réelle, un nombre important de ce type d'infraction étant toujours détecté. Il convient toutefois de noter que ces chiffres étaient inférieurs aux premier et deuxième trimestres 2022 par rapport à 2021. Cette baisse peut s'expliquer par divers facteurs, mais le plus probable est le nombre record de détections au mois de mars. Ce pic semble principalement lié à un grand nombre de détections de la famille de rançongiciels Conti en Tunisie, dont la neutralisation peut avoir entraîné une chute des détections au mois d'avril, selon Trend Micro.

<sup>14</sup> The State of Ransomware 2022 (<https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf>)

<sup>15</sup> Remarks by Deputy Secretary of the Treasury (<https://home.treasury.gov/news/press-releases/jy1067>)

## DÉTECTIONS DE RANÇONGIELS



SOURCE: TREND MICRO

Dans un autre rapport, Trend Micro a indiqué que les cinq secteurs les plus fréquemment touchés étaient les organismes publics, l'éducation, l'énergie, le commerce de détail et les produits de grande consommation. Un autre rapport observe que les infrastructures critiques telles que la santé et le transport sont également ciblées.

Les outils de protection des données et de sauvegarde se sont perfectionnés au fil du temps, ce qui a progressivement sapé l'efficacité des attaques par rançongiciel traditionnelles. Lorsqu'une organisation dispose d'une sauvegarde des données cryptées, elle n'a pas besoin de payer la rançon demandée par les cybercriminels. Ces derniers doivent ainsi faire preuve de créativité et développer des doubles ou triples rançongiciels.

La dernière évolution en date est l'essor des rançongiciels en tant que service (RaaS), qui

permettent aux cybercriminels de louer des versions prédéveloppées de rançongiciels pouvant être utilisées pour mener des attaques.

Grâce aux RaaS, il est plus facile que jamais pour les cybercriminels de mener à bien des attaques par rançongiciel : ils n'ont même plus besoin d'avoir des compétences techniques et une expérience poussées. Par ailleurs, ce type de service permet de cibler facilement un grand nombre de victimes en même temps du fait de son extensibilité et de sa flexibilité. Les cybercriminels adaptent leurs techniques en fonction de ce qui marche le mieux dans chaque cas, étant donné qu'ils peuvent rapidement passer d'une version de rançongiciel à une autre. Toutes ces caractéristiques exacerbent la dangerosité des RaaS, car les cybercriminels n'ont plus besoin de disposer de compétences et d'infrastructures complexes pour mener à bien des attaques.

Les données transmises par 42 pays de la région africaine révèlent que seules 59 attaques par rançongiciel ont été signalées aux services chargés de l'application de la loi dans 11 pays africains. La situation réelle est certainement bien pire : de nombreux particuliers et entreprises étant réticents à signaler ces cas à la police, l'on estime qu'un faible pourcentage d'attaques par rançongiciel sont rendues publiques.

Les raisons pour lesquelles ces attaques ne sont pas signalées sont, pour les particuliers, la crainte que les données cryptées perdent de la valeur et, pour les entreprises, qu'elles ne souhaitent pas que leurs clients sachent que leurs données ont été corrompues, une préoccupation bien plus grave pour les entreprises. Les victimes taisent généralement ce type d'incident et paient la rançon, tandis que les cybercriminels ne publient pas toujours les données issues des réseaux corrompus.

## 2.4 Chevaux de Troie bancaires et voleurs d'informations

L'Afrique connaît actuellement un essor spectaculaire dans le secteur des technologies numériques, en particulier s'agissant des technologies de la finance et du commerce électronique. Cette croissance s'explique par un accès accru à Internet et une meilleure pénétration des technologies mobiles, qui permettent à la population d'accéder à des services auparavant hors de portée. Cela a créé des opportunités de croissance et de développement des activités économiques à travers le continent.

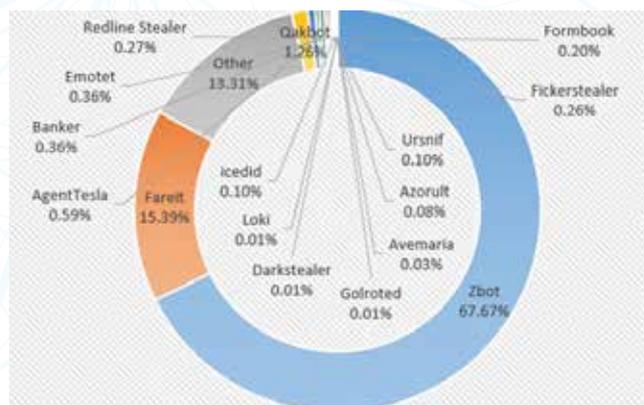
Néanmoins, cet essor rapide facilite les attaques via des logiciels malveillants comme les chevaux de Troie bancaires et les voleurs d'informations, qui représentent l'une des plus graves menaces, à la fois pour la sécurité des particuliers et pour les infrastructures informatiques des organisations, en raison de leur capacité à causer des dommages considérables s'ils ne sont pas détectés à temps.

Les chevaux de Troie bancaires et les voleurs d'informations peuvent être installés manuellement ou à distance via des techniques d'ingénierie sociale comme des courriels contenant des liens ou pièces jointes malveillants. Une fois installés, ils recueillent des informations personnelles sur l'ordinateur infecté et transmettent ces données volées à un serveur distant contrôlé par le cybercriminel.

Celui-ci peut ensuite utiliser les informations obtenues pour dérober de l'argent à la victime, ou les vendre sur des marchés clandestins.

Comme le révèlent les détections de Trend Micro, le Maroc est le pays africain le plus touché, avec pas moins de 18 827 détections. L'Afrique du Sud n'est pas loin derrière, avec 6 560 détections de logiciels malveillants. S'ensuivent le Nigéria (5 366 détections), le Cameroun (1 462 détections) et l'Algérie (691 détections).

Des rapports indiquent par ailleurs que les principaux chevaux de Troie bancaires et voleurs d'informations sont Zbot et Fareit. Le premier représente 67,67 % des détections dans la région et le second, 15,39 %. L'utilisation de ces deux logiciels malveillants s'est inscrite en hausse ces dernières années en Afrique, ciblant tant les entreprises que les particuliers.



Zbot et Fareit sont tous deux difficiles à détecter et parviennent souvent à voler des informations personnelles et financières à leurs victimes avant même qu'elles ne se rendent compte de l'attaque, ce qui engendre des pertes considérables.

Un autre voleur d'informations à surveiller dans la région africaine est RedLine Stealer : les recherches menées par Group-IB révèlent qu'entre janvier et août 2022, pas moins de 5 862 188 comptes corrompus associés à des adresses IP africaines ont été obtenus via RedLine Stealer.

Il a été démontré que ce voleur d'informations était généralement diffusé via des jeux, applications et services piratés dans le but de voler des informations sensibles telles que les données du navigateur, les portefeuilles de cybermonnaies et les identifiants d'utilisateur de programmes populaires comme FileZilla, Discord, Steam, Telegram et les VPN.

Les chevaux de Troie bancaires et les voleurs d'informations représentent une réelle menace en Afrique, qui doit être prise au sérieux afin de protéger les citoyens des pertes financières engendrées par le vol de fonds ou l'usurpation d'identité. La population marocaine est particulièrement exposée aux chevaux de Troie bancaires, comme l'indique le grand nombre de logiciels malveillants détectés dans le pays ; les citoyens des autres pays africains doivent toutefois rester vigilants et mettre régulièrement à jour leurs dispositifs de sécurité en ligne pour prévenir les éventuelles attaques. Il convient de noter que ces chiffres n'incluent pas les cas d'escroquerie qui n'ont pas été détectés ou signalés ; l'ampleur réelle du préjudice causé par les chevaux de Troie bancaires peut donc être bien plus importante que les statistiques ne le laissent à penser.

Les banques et les établissements financiers doivent instaurer des mesures pour protéger leurs clients des cyberinfractions comme le hameçonnage et les infections par des logiciels malveillants, mais il incombe également aux particuliers d'être prudents lorsqu'ils réalisent des opérations financières via Internet. La mise à jour régulière des antivirus et des outils de protection contre les logiciels malveillants sur les appareils constitue la première ligne de défense contre certaines menaces comme les chevaux de Troie bancaires. Les utilisateurs doivent par ailleurs définir des mots de passe uniques et difficiles à deviner par les cybercriminels afin de garantir une sécurité maximale. Enfin, une action collective des banques, des organismes publics et des utilisateurs est nécessaire pour enrayer la tendance cybercriminelle liée aux chevaux de Troie bancaires en Afrique.

## 2.5 Escroqueries en ligne et extorsion

Les escroqueries en ligne comprennent un vaste éventail d'activités frauduleuses dans la sphère numérique. Les escroqueries par défaut de livraison avec paiement anticipé, les escroqueries commerciales, les escroqueries aux sentiments, la sextorsion, les escroqueries à l'assistance technique et les escroqueries aux cybermonnaies figurent parmi les escroqueries en ligne les plus courantes et gagnent du terrain dans la région africaine. Les escroqueries avec paiement anticipé consistent à demander un acompte avant de livrer des produits ou de fournir des services. Les criminels recourent généralement à cette stratégie pour obtenir de

l'argent auprès de personnes non averties, puis disparaissent sans livrer les produits ou fournir les services. Aux fins de vraisemblance, les escrocs peuvent également envoyer de faux documents ou demander des informations personnelles comme des coordonnées bancaires, des numéros de compte bancaire et des adresses courriel.

Les escroqueries aux sentiments consistent à créer un lien affectif avec une personne non avertie sous couvert d'une fausse identité sur une plateforme de médias sociaux ou un site de rencontre. Après avoir gagné sa confiance et obtenu l'accès à ses comptes personnels, le criminel exploite cette relation pour réclamer de l'argent à sa victime sous de faux prétextes, ou pour voler des informations sensibles telles que des mots de passe et des coordonnées bancaires.

La sextorsion est une autre forme préoccupante d'escroquerie en ligne : c'est une forme hybride d'escroquerie aux sentiments qui consiste à faire chanter des victimes en les menaçant de diffuser des photos ou vidéos intimes si elles ne paient pas une rançon.

Les escroqueries à l'assistance technique sont un type d'escroquerie qui consiste à se faire passer pour des représentants de sociétés de technologie proposant un service d'assistance technique en vue d'accéder à l'ordinateur des utilisateurs et d'en extraire des données précieuses comme des mots de passe et des informations financières. Les criminels peuvent avoir recours à diverses stratégies telles que le démarchage, les pop-ups publicitaires, les faux courriels ou les messages automatiques prétendant que l'ordinateur des utilisateurs est infecté par un logiciel malveillant afin de les amener à autoriser l'accès à distance à leur système.



Les escroqueries aux cybermonnaies tirent parti de la popularité croissante des cybermonnaies comme le bitcoin et l'éthereum en incitant des investisseurs à acquérir de fausses devises. Ces escrocs recourent à des tactiques complexes comme la création de faux portefeuilles et de fausses opérations de change en vue de dérober des fonds auprès de victimes non averties.

Les plateformes de médias sociaux, qui comptent des milliards d'utilisateurs et dont l'utilisation quotidienne explose, constituent une cible lucrative pour les cybercriminels et les escrocs.

Bien que la perception des médias sociaux ait changé ces dernières années, le comportement des utilisateurs n'a pas évolué pour autant. Bon nombre d'entre eux ne savent toujours pas réellement comment sont traitées leurs informations personnelles, ce qui les rend vulnérables face à des individus malveillants. Les cybercriminels recourent à la tromperie via des courriels de hameçonnage ou des liens malveillants pour accéder aux comptes des utilisateurs et voler des données sensibles, ou pirater des comptes aux fins d'usurpation d'identité. Les escroqueries sont pléthore sur les plateformes de médias sociaux, des fausses offres d'emploi aux systèmes pyramidaux et autres escroqueries aux placements. Malheureusement, ces escroqueries ciblent généralement des personnes rencontrant

déjà des difficultés financières et étant donc plus exposées aux pertes financières et à la détresse psychologique. Les escrocs particulièrement habiles peuvent même pirater des comptes d'utilisateur ou créer de faux comptes pour envoyer des liens malveillants ou des messages contenant des logiciels malveillants.

Les cybercriminels tirent également parti du large public mondial accessible via ces plateformes en adaptant les escroqueries en fonction de la localisation des utilisateurs. Cette tactique leur permet de propager rapidement et facilement de la désinformation, amenant des personnes à croire à de fausses actualités ou à investir dans des mécanismes frauduleux. De plus, certains individus malveillants exploitent le caractère interactif des médias sociaux en se faisant passer pour des personnalités célèbres ou des sociétés renommées en vue de gagner en crédibilité et de toucher plus de victimes.



Ces formes de cyberinfractions sont particulièrement prolifiques dans la région africaine en raison d'un manque d'information du grand public quant à leur existence et leur fonctionnement. Au vu de l'évolution rapide des technologies, il peut s'avérer difficile de suivre le rythme des tendances en matière de cybercriminalité et de détecter les éventuels signaux de danger pour éviter de tomber dans le piège. Par ailleurs, les personnes rencontrant des difficultés financières sont souvent plus susceptibles d'accepter les offres d'escrocs en pensant qu'elles vont les sortir d'affaire, alors que c'est tout le contraire. Il est ainsi essentiel pour les pouvoirs publics et les services chargés de l'application de la loi de prendre des mesures proactives en matière d'information des citoyens sur les diverses formes d'escroqueries en ligne et leur fonctionnement, ainsi que sur les mesures à prendre pour s'en prémunir.

Les conséquences de ces cyberinfractions peuvent être dévastatrices : non seulement les victimes perdent de l'argent, mais elles peuvent également se faire usurper leur identité et leur vie en est détruite. Ce type d'escroqueries est souvent mené à l'échelle internationale : les pirates informatiques créent de faux comptes dans plusieurs pays en quelques clics, qui leur permettent de commettre discrètement des infractions aux dépens de victimes non averties à travers le monde. Les utilisateurs

doivent donc impérativement rester vigilants lorsqu'ils naviguent sur Internet pour éviter de tomber dans le piège. Les médias sociaux doivent également prendre des mesures proactives afin de protéger leurs utilisateurs de ce type d'activités malveillantes, en renforçant leurs dispositifs de sécurité pour combler les failles de leurs systèmes pouvant être exploitées par les criminels.

Si ces cyberinfractions semblent être orchestrées grâce à l'ingénierie sociale, les chercheurs de Trend Micro ont identifié 7,7 millions de détections de sites malveillants, dont la plupart concernant des escroqueries (40,31 %). Il a également été constaté que les courriers indésirables aux fins d'extorsion constituaient une méthode de cyberattaque plébiscitée à travers le monde. Sur l'ensemble des pays africains étudiés, 69,24 % (13 002) des courriels d'extorsion ont été détectés au Maroc.

Si l'on s'intéresse à la répartition mondiale des détections identifiées par Trend Micro, 2,44 % des adresses IP des expéditeurs étaient géolocalisées en Afrique du Sud, 2,13 % au Maroc, 0,94 % au Kenya et 0,91 % en Tunisie, ce qui suggère que ces serveurs ont été corrompus ou font partie d'un réseau de machines zombies destiné à des activités malveillantes comme des campagnes de courriers indésirables aux fins d'extorsion. Il est fort probable que les cybercriminels exploitent les failles de ces



serveurs pour en prendre le contrôle et mener des activités malveillantes telles que la propagation de logiciels malveillants et le lancement d'attaques par hameçonnage.

Face à un environnement cybercriminel en constante évolution, les communautés mondiales des services chargés de l'application de la loi et de la cybersécurité ont formé une alliance afin de protéger les populations.

Mettant à profit l'expertise de cette alliance, INTERPOL a lancé plusieurs campagnes de sensibilisation mondiale (#ÇaN'arrivePasQu'AuxAutres, #JustOneClick, #OnlineCriminalsRealCrime) en vue d'informer les populations des cybercriminels qui cherchent à exploiter, à voler des données, à commettre des escroqueries sur Internet, ou tout simplement à perturber le monde virtuel.

## 2.6 Logiciels criminels en tant que service

Le modèle CaaS (logiciels criminels en tant que service) n'est pas nouveau pour les experts en cybersécurité, les services chargés de l'application de la loi et les autres acteurs de la sécurité numérique. Il permet aux cybercriminels de proposer des codes malveillants en tant que « service » à d'autres criminels, qui les utilisent pour infecter des ordinateurs, voler des données, puis monétiser leurs activités illégales.

Ce mode opératoire du milieu criminel a révolutionné les méthodes d'intervention des cybercriminels, qui ont désormais facilement accès à des outils et services difficiles à trouver, tels que des réseaux de machines zombies, des rançongiciels en tant que service, ou encore des ressources permettant de mener des attaques par DDoS. Par ailleurs, grâce à l'adoption d'un modèle d'entreprise, les criminels sont de plus en plus organisés et peuvent accroître aussi bien leurs capacités techniques que leurs bénéfices.

En proposant des logiciels criminels via un modèle CaaS, les cybercriminels mettent à disposition un vaste éventail de variantes de logiciels malveillants à un prix abordable. La facilité avec laquelle il est possible d'acheter ou de s'abonner à ces services, voire de les utiliser à la demande, permet de déployer rapidement des logiciels malveillants à l'échelle mondiale, sans même disposer de

connaissances techniques particulières. Ces services garantissent généralement l'anonymat total de bout en bout du processus de transaction.

Tandis que les cyberinfractions traditionnelles sont souvent limitées par les contraintes géographiques ou la lenteur des connexions Internet, susceptibles de restreindre l'accès ou de retarder fortement la mise en œuvre, les modèles CaaS récents qui s'appuient sur les technologies dématérialisées ont radicalement changé la donne, puisqu'ils permettent de déployer des logiciels malveillants en quelques minutes aux quatre coins du monde. Cela réduit considérablement les coûts d'exploitation pour les criminels, qui peuvent ainsi cibler des victimes plus rapidement et plus efficacement.

Cette approche élimine en outre une grande partie du risque lié aux méthodes traditionnelles d'achat de logiciels malveillants. Étant donné que toutes les transactions s'effectuent en ligne au moyen de cybermonnaies ou de modes de paiement similaires, le risque d'être repéré est beaucoup plus faible. Cet aspect constitue une source de motivation supplémentaire pour les criminels désireux de saisir les opportunités lucratives offertes par le modèle CaaS sans craindre de se faire prendre.

Globalement, les CaaS ont assoupli les barrières à l'entrée pour les cybercriminels en herbe, qui peuvent mener des attaques complexes sans même disposer de compétences techniques poussées. Les CaaS s'affichent partout sur les forums et marchés criminels du Darknet comme une gamme de services bon marché et facilement accessibles. Ils sont également présentés comme la solution idéale pour les cybercriminels chevronnés qui souhaitent lancer des campagnes éclair.

Autre élément intéressant pour les cybercriminels en quête de nouveaux défis ou de nouvelles cibles, les logiciels criminels en tant que service permettent d'utiliser les données volées pour mener des attaques ultérieures.

Le modèle CaaS complique l'attribution d'une infraction à un individu en particulier car les moyens et infrastructures sont partagés entre plusieurs criminels ou groupes. Il est particulièrement dangereux car il sert de facilitateur pour des attaques de plus en plus complexes, qui alimentent l'essor rapide de nouvelles menaces avancées.

	 Kits de hameçonnage	 Hameçonnage en tant que service (PaaS)
	Ponctuel	Abonnement (hebdomadaire, bimensuel, mensuel ou annuel)
Paiement		
Modèles de courriels	✓	✓ (en option)
Modèles de sites	✓	✓
Diffusion de courriels		✓ (en option)
Hébergement de site		✓
Vol d'identifiants		✓
Redistribution d'identifiants		✓
Liens/journaux « 100 % indétectables »		✓

### Comparaison des fonctionnalités entre les kits de hameçonnage et le hameçonnage en tant que service.

Source: Microsoft

En alliant ces différents types d'attaque, les cybercriminels peuvent mettre à mal les capacités et les moyens des services chargés de l'application de la loi en matière d'enquête et d'attribution des attaques à un/des individu(s) ou groupe(s) en particulier.

Le hameçonnage en tant que service (PaaS) propose des campagnes de hameçonnage automatiques et plus longues, qui peuvent être déployées rapidement et à moindre coût. Il suffit de payer en bitcoin pour avoir accès à des réseaux de machines zombies ; une multitude de machines infectées par des logiciels malveillants à travers le monde vont ensuite lancer de puissantes attaques par DDoS contre les cibles choisies, selon la capacité réseau et la durée souhaitées.

Ces dernières années, les attaques par rançongiciel ont connu une hausse sans précédent, qui s'explique principalement par la mise à disposition de rançongiciels en tant que service (RaaS) prêts à l'emploi. Ils permettent en effet aux utilisateurs de mener plusieurs campagnes sans même devoir écrire du code. Les plateformes de RaaS se présentent sous forme de portails en ligne conviviaux proposant des services d'assistance et des abonnements à prix intéressant. En règle générale, elles prennent entre 20 et 40 % des rançons collectées.

Le recours accru à ces outils cybercriminels a entraîné une explosion des activités malveillantes sur Internet ainsi qu'une amplification des pertes liées à ce type d'infractions. Il n'est en outre pas rare que les criminels collaborent en partageant leur expertise technique et leurs ressources via des forums spécifiques afin d'accroître les chances de réussite de leurs cyberattaques. Par ailleurs, certains de ces services fournissent des renseignements sur les menaces qui permettent aux utilisateurs de cibler des organisations ou segments de clientèle en particulier afin d'accroître les chances de réussite d'une campagne de hameçonnage. Étant donné la facilité avec laquelle il est possible de lancer ce type d'attaque et leur rentabilité, il ne fait aucun doute que les cybercriminels continueront à utiliser les RaaS malgré les risques encourus.

Au vu du nombre croissant de CaaS proposés sur des forums cybercriminels et de piratage, notamment ceux sur le Darknet, il est primordial de surveiller ces plateformes en vue d'identifier les nouvelles menaces le plus tôt possible et d'échanger rapidement des informations pour les détecter et limiter les risques représentés par les cyberattaques.

### 3. BRÈVE PRÉSENTATION DES CAPACITÉS EN MATIÈRE DE CYBERCRIMINALITÉ DANS LA RÉGION AFRICAINE

En vue de lutter efficacement contre la cybercriminalité, les services chargés de l'application de la loi de la région africaine ont besoin de systèmes de cybersécurité robustes et correctement structurés. L'instauration de politiques, d'une législation et de services spécialisés est nécessaire pour apporter une réponse adéquate aux innombrables cybermenaces et incidents auxquels les pays du monde entier sont confrontés ; il convient d'en faire une priorité absolue.

Les données transmises par les 42 pays africains interrogés révèlent que la majorité d'entre eux disposent de politiques, d'une législation et de services spécialisés en matière de cybercriminalité permettant d'apporter une réponse adéquate aux innombrables cybermenaces auxquels les pays du monde entier sont confrontés.

Cependant, huit pays ont indiqué ne pas disposer d'une unité spécialisée dans les cyberinfractions, et sept ont indiqué ne pas avoir instauré de législation en matière de cybercriminalité.

La faiblesse de la législation en matière de cybercriminalité (voire son inexistence dans certains pays) laisse le champ libre aux criminels qui peuvent agir en toute impunité, puisque, même s'ils se font prendre, ils ne sont pas poursuivis ni extradés vers des pays disposant d'une législation plus stricte.

Afin de suivre le rythme de l'évolution des cyberinfractions et des actes criminels ciblant les systèmes informatiques, il est fortement recommandé que les pays de la région africaine poursuivent l'examen de la législation actuelle en matière de cybercriminalité et l'actualisent régulièrement, au gré des avancées technologiques.

Il va également de soi que les unités spécialisées dans la cybercriminalité sont probablement les plus efficaces en matière de prévention, de détection, d'enquête et de poursuites des cyberinfractions pour les citoyens et les entreprises. En effet, si les pouvoirs publics souhaitent fournir un service concret au grand public qui réponde à leurs attentes et à leurs besoins, ils doivent notamment se doter d'une unité d'enquête spécialisée dans la cybercriminalité.

L'utilisation accrue des technologies s'accompagne d'un risque accru de détournement de ces technologies par les criminels. Cet état de fait est largement admis par toutes les entités concernées. Bien qu'une majorité des services chargés de l'application de la loi de la région africaine aient créé ou renforcé une ou plusieurs unités spécialisées dans la cybercriminalité, il apparaît clairement que leurs capacités demeurent limitées face aux cyberinfractions complexes. De plus, la région africaine couvre une vaste zone géographique, et les initiatives sont insuffisantes pour développer les capacités des enquêteurs spécialisés dans la cybercriminalité à l'échelle locale.

Dans un environnement où l'économie est florissante, il existe plusieurs solutions à étudier par les services chargés de l'application de la loi et les organismes concernés. Une stratégie ou un plan d'action intégré et coordonné en matière de cybercriminalité pourrait définir la vision, les objectifs et les priorités de la lutte contre la cybercriminalité, tant directement via une action répressive qu'indirectement via une collaboration intergouvernementale et la formation de partenariats avec les secteurs public et privé, aux niveaux national et international, pour créer un environnement virtuel résilient et fiable.

Le but est d'éviter la duplication des initiatives et de résoudre les problèmes notamment liés au contenu et à la réglementation d'Internet, dans l'optique d'instaurer un cadre stratégique à long terme permettant d'étudier les difficultés et les opportunités, puis de définir des axes prioritaires sur lesquels les pays doivent concentrer leurs efforts en matière de cybersécurité et de lutte contre la cybercriminalité au bénéfice de l'ensemble des parties prenantes (ex. prévention de la cybercriminalité et promotion d'une bonne hygiène informatique et des pratiques de sécurité auprès du grand public).

Le taux de cyberinfractions et d'infractions commises à l'aide d'Internet s'inscrit en hausse à l'échelle mondiale, ce qui n'échappe pas aux services chargés de l'application de la loi, qui investissent souvent massivement dans un grand nombre d'affaires et élargissent les unités d'enquête spécialisées dans la cybercriminalité.

Du côté de la direction, il est également admis que les unités spécialisées dans la cybercriminalité sont probablement les plus efficaces en matière de prévention, de détection, d'enquête et de poursuites des cyberinfractions au bénéfice des citoyens et des entreprises. En effet, si les pouvoirs publics souhaitent fournir un service concret au grand public qui réponde à leurs attentes et à leurs besoins, ils doivent notamment se doter d'une unité d'enquête spécialisée dans la cybercriminalité.

Les services chargés de l'application de la loi doivent par ailleurs envisager d'investir dans le renforcement de leurs capacités en matière de lutte contre les cyberinfractions et les infractions commises à l'aide d'Internet, mais aussi dans l'amélioration de l'efficacité des sections/unités d'enquête générales et spécialisées dans la cybercriminalité, notamment via :

- l'examen des capacités des unités d'enquête spécialisées dans la cybercriminalité et dans la criminalistique numérique ;
- le recours à des outils comme l'analyse des mégadonnées et le crypto-traçage ;
- la création de relations externes avec les acteurs majeurs du secteur en vue d'accroître l'échange d'informations et d'expertise ;
- l'élaboration de POS en matière d'enquête et de criminalistique ;
- la centralisation des outils de criminalistique numérique sous la forme d'un centre de services à disposition de toutes les unités de police, favorisant la transmission de connaissances et la spécialisation individuelle, mais aussi des gains d'efficacité en termes d'approvisionnement ;
- le développement d'une plateforme de formation en ligne axée sur la cybercriminalité et les éléments de preuve numériques aux fins d'évolutivité.

La prévention sera toujours la première et la meilleure ligne de défense contre les cybercriminels. À l'instar d'autres activités criminelles, les personnes les plus vulnérables sont souvent les premières ciblées. Les campagnes d'information et de sensibilisation contribuent grandement à protéger les personnes vulnérables contre diverses formes de cybercriminalité.

Si la plupart des pays de la région africaine mènent des initiatives de sensibilisation à et de prévention de la cybercriminalité, 10 pays ont indiqué n'en mener aucune. Il y a donc encore fort à faire dans ce domaine pour obtenir les meilleurs résultats.

Étant donné qu'une grande partie de la population utilise les plateformes de médias sociaux comme Facebook, WhatsApp, Instagram, Twitter, etc., il pourrait être utile de créer une page spécifique via laquelle les services chargés de l'application de la loi prodigueraient des conseils en matière de prévention de la cybercriminalité au grand public et recueilleraient des informations sur les cyberinfractions.

## 4. MARCHE À SUIVRE : ACTION PROACTIVE FACE À L'ÉVOLUTION DES CYBERMENACES DANS LA RÉGION AFRICAINE

Nous avons évoqué les diverses cybermenaces et tendances représentant un risque pour la région africaine, mais il convient également d'approfondir la connaissance et la compréhension des menaces auxquelles la région va être confrontée à l'avenir. Les cyberstratégies ont tendance à se concentrer sur des mesures réactives en vue d'empêcher les cyberattaques (rançongiciels, hameçonnage, escroqueries aux FOVI, logiciels malveillants). Néanmoins, étant donné que les cybercriminels agissent, vendent et partagent leurs connaissances principalement sur le Darknet, les services chargés de l'application de la loi et les équipes de cybersécurité des entreprises doivent être proactifs en matière de recueil et d'analyse de renseignements sur les menaces externes, ainsi que de détection des cybermenaces avant qu'elles ne se transforment en attaques.

Le recueil de renseignements est une pièce essentielle du puzzle ; INTERPOL fournit un appui à ses pays membres dans ce domaine afin de juguler l'évolution des cybermenaces en créant des capacités comme le Desk africain pour les opérations de lutte contre la cybercriminalité. Ce dernier, soutenu par l'unité Cyber-renseignement d'INTERPOL, partage des renseignements sur les cybermenaces et coordonne des opérations conjointes auxquelles participent des entités publiques et privées. Il est impératif de connaître les techniques d'attaque et le moment où des individus malveillants prévoient de passer à l'action pour contrecarrer les cyberattaques en amont de la chaîne de frappe.

Dans un monde toujours plus numérique, plus les pays ont connaissance tôt d'une menace, plus vite ils peuvent prendre des mesures pour atténuer les risques et endiguer les cybermenaces.

Par ailleurs, les services chargés de l'application de la loi doivent renforcer l'action collective en termes de partage de renseignements et d'instauration d'un cadre opérationnel conjoint pour lutter efficacement contre la cybercriminalité dans la région africaine.

Bien que les services chargés de l'application de la loi du continent entretiennent de bonnes relations et aient conclu des accords de coopération bilatéraux pour lutter contre les infractions traditionnelles,

un cadre opérationnel de lutte contre la cybercriminalité fait encore défaut.

En vue d'accroître l'efficacité des opérations conjointes à l'échelle tant intrarégionale qu'interrégionale, le Desk africain pour les opérations de lutte contre la cybercriminalité a formulé un cadre opérationnel baptisé « Cadre opérationnel conjoint pour l'amélioration des actions coordonnées contre la cybercriminalité dans la région africaine ».

Ce cadre orientera les opérations menées par INTERPOL avec la communauté des services chargés de l'application de la loi dans la région africaine, en indiquant comment élaborer, coordonner et communiquer lors d'opérations conjointes pour garantir un échange rapide et efficace d'informations. Il prône en particulier une réelle coopération entre les services chargés de l'application de la loi, les organisations internationales/intergouvernementales et le secteur privé.

En prévision du développement de nouvelles politiques et de cadres législatifs dans les pays africains, il s'agira d'un document évolutif qui sera adapté en vue de garantir sa pertinence et sa cohérence avec les normes régionales et internationales en vigueur.

## 5. CYCLE ANNUEL DE PLANIFICATION DU DESK AFRICAIN POUR LES OPÉRATIONS DE LUTTE CONTRE LA CYBERCRIMINALITÉ

En vue d'atteindre ses objectifs, le Cadre opérationnel conjoint pour l'Afrique propose un cycle annuel de planification en quatre étapes afin de promouvoir une approche cohérente et méthodique en matière de perfectionnement des opérations proactives coordonnées contre la cybercriminalité dans la région.

### Étape I : Recueil et analyse

La première étape concerne l'analyse approfondie des informations relatives aux principales cybermenaces, aux infrastructures malveillantes et aux cybercriminels ciblant la population dans la région africaine. Le Desk africain pour les opérations de lutte contre la cybercriminalité s'appuiera sur les renseignements communiqués par les services chargés de l'application de la loi, les recherches menées par l'unité Cyberrenseignement d'INTERPOL et les divers accords de partage de données conclus avec les partenaires du projet Gateway d'INTERPOL en vue d'élaborer le Rapport d'évaluation des cybermenaces en Afrique, qui permettra aux services chargés de l'application de la loi de la région d'approfondir leur compréhension du contexte des cybermenaces.

### Étape II : Priorités et stratégie

Le Rapport d'évaluation des cybermenaces en Afrique publié au cours de l'étape I servira de document de référence pour les pays membres africains dans le cadre de l'élaboration et de l'actualisation de leurs stratégies et méthodes d'enquête, et orientera la priorisation régionale des opérations menées conjointement avec INTERPOL pour l'année à venir. L'Afrique est une région diversifiée et chaque pays est confronté à ses propres défis ; le Desk africain pour les opérations de lutte contre la cybercriminalité sollicitera donc le chef de l'unité Cybercriminalité de chaque pays (avec l'autorisation de son B.C.N.) lors de cette étape en vue d'étudier les possibilités de collaboration tant intrarégionale qu'interrégionale. À l'issue de cette étape, une feuille de route régionale fondée sur une stratégie commune et définissant clairement les résultats opérationnels pour l'année sera prête à être publiée.

### Étape III : Opérations

Le Desk africain pour les opérations de lutte contre la cybercriminalité élaborera des plans tactiques standard (PTS) pour mettre en œuvre la stratégie convenue lors de l'étape II. Les PTS définissent clairement les objectifs, les fonctions et les responsabilités, ainsi qu'un concept opérationnel en matière de lutte contre certaines cybermenaces. Chaque PTS comprend généralement un plan détaillé concernant 1) la planification et l'analyse, 2) l'organisation, 3) la tactique et 4) l'évaluation. Il est ensuite soumis à l'approbation des pays participants.

Les unités spécialisées dans la cybercriminalité désignées par le B.C.N. s'engageront alors à mener les actions décrites dans le PTS et apporteront tout leur soutien à la réalisation des buts et objectifs opérationnels convenus. Une fois le PTS approuvé, les opérations seront coordonnées par le Desk africain pour les opérations de lutte contre la cybercriminalité et menées par les enquêteurs désignés selon le calendrier défini dans le PTS. Les données relatives aux opérations seront transmises à INTERPOL pour analyse via son système de communication sécurisé I-24/7 ou sa Plateforme collaborative sur la cybercriminalité - Opérations.

À réception des informations opérationnelles, les points de contact désignés de chaque pays membre se mettront en relation avec le Desk africain pour les opérations de lutte contre la cybercriminalité en vue d'échanger des informations selon les objectifs fixés et le calendrier de l'opération. Le pays membre à l'origine de l'opération en assurera la direction de bout en bout.

La conservation et la diffusion des relevés Internet (informations élémentaires sur les abonnés, données de transmission, contenu, etc.) se feront sur la base du volontariat et seront encouragées dans le cadre des opérations menées en matière de cybercriminalité, au vu de la nature volatile des éléments de preuve électroniques. Dans la mesure autorisée par leurs lois et politiques, les pays membres seront fortement invités à communiquer les avancées des enquêtes et les renseignements spécifiques susceptibles d'aider d'autres pays membres pour leurs propres enquêtes. Dans la mesure du possible, les points de contact devront faciliter l'échange d'informations avec d'autres services nationaux tels que les équipes d'intervention informatique d'urgence (CERT) et les banques centrales, en fonction des besoins de chaque opération.

### Étape IV : Évaluation

Au cours de l'étape IV, un rapport de retour d'expérience (RRE) sera dressé afin d'identifier les enseignements tirés des opérations. Le Desk africain pour les opérations de lutte contre la cybercriminalité recommandera des ajustements pour les futures opérations conjointes en s'appuyant sur ce rapport et les nouvelles informations issues des opérations. Les renseignements recueillis lors de l'étape III seront également évalués en vue d'approfondir la compréhension régionale des principales cybermenaces et d'alimenter le prochain Rapport d'évaluation des cybermenaces en Afrique.



# INTERPOL

Complexe mondial INTERPOL pour l'innovation  
18 Napier Road  
Singapour 258510

SUIVEZ-NOUS:



INTERPOL



YouTube

INTERPOLHQ



INTERPOL\_HQ



@INTERPOL\_HQ



INTERPOL HQ



[www.interpol.int](http://www.interpol.int)